Why we are failing and how we can fix this

MOBILE DEVICES

Your presenter: Michael Robinson

michael.robinson@disruptive-sol.com

Disruptive Solutions
Director of Forensics

Stevenson University
Program Coordinator, Cyber Forensics

George Mason University
Adjunct Professor

The graphic artists have been busy.

Malware

KILL

TROJAN ALERT

ER'T

DROID

But does popular opinion make it real?

Who is using them?

	Population	Cell Phones
World	7.0 billion	> 6.8 billion
China	1.35 billion	1.28 billion
India	1.22 billion	1.10 billion
US	318 million	328 million
Russia	143 million	256 million
Brazil	201 million	274 million
Indonesia	238 million	237 million
Pakistan	181 million	132 million

CTIA: The Wireless Association
The International Association for the Wireless Telecommunications Industry
http://www.ctia.org

In the United States

	Dec 2010	Dec 2011	Dec 2012
Wireless only households	26.6%	34%	35.8%
Annual minutes of use	2,200,000,000,000	2,296,000,000,000	2,300,000,000,000
Monthly text messages	175,000,000,000	193,100,000,000	171,300,000,000
Annual text messages	2,100,000,000,000	2,300,000,000,000	2,190,000,000,000
Annual MMS messages	56,600,000,000	58,300,000,000	-
Wireless data	-	866,700,000,000 MB	1,468,000,000,000 MB
911 calls from cell phones	> 296,000 per day	> 396,000 per day	> 400,000 per day
Cell sites	253,086	283,385	301,779

Top four states for adults and children living in wireless-only households are: Idaho (44.6%); Arkansas (44.4%); Mississippi (42.3%); North Dakota (41.6%).

Prepaid/Pay-As-You-Go services' share of overall wireless market (penetration) is 23.4%, equal to more than 76.4 million wireless prepaid/pay-as-you-go subscribers as of December 2012.

There are 630+ different handsets and devices manufactured for the U.S. market.

http://www.ctia.org/advocacy/research/index.cfm/AID/10378

Android Activation Rate

http://www.businessinsider.com/chart-of-the-day-android-activations-per-day-2012-9

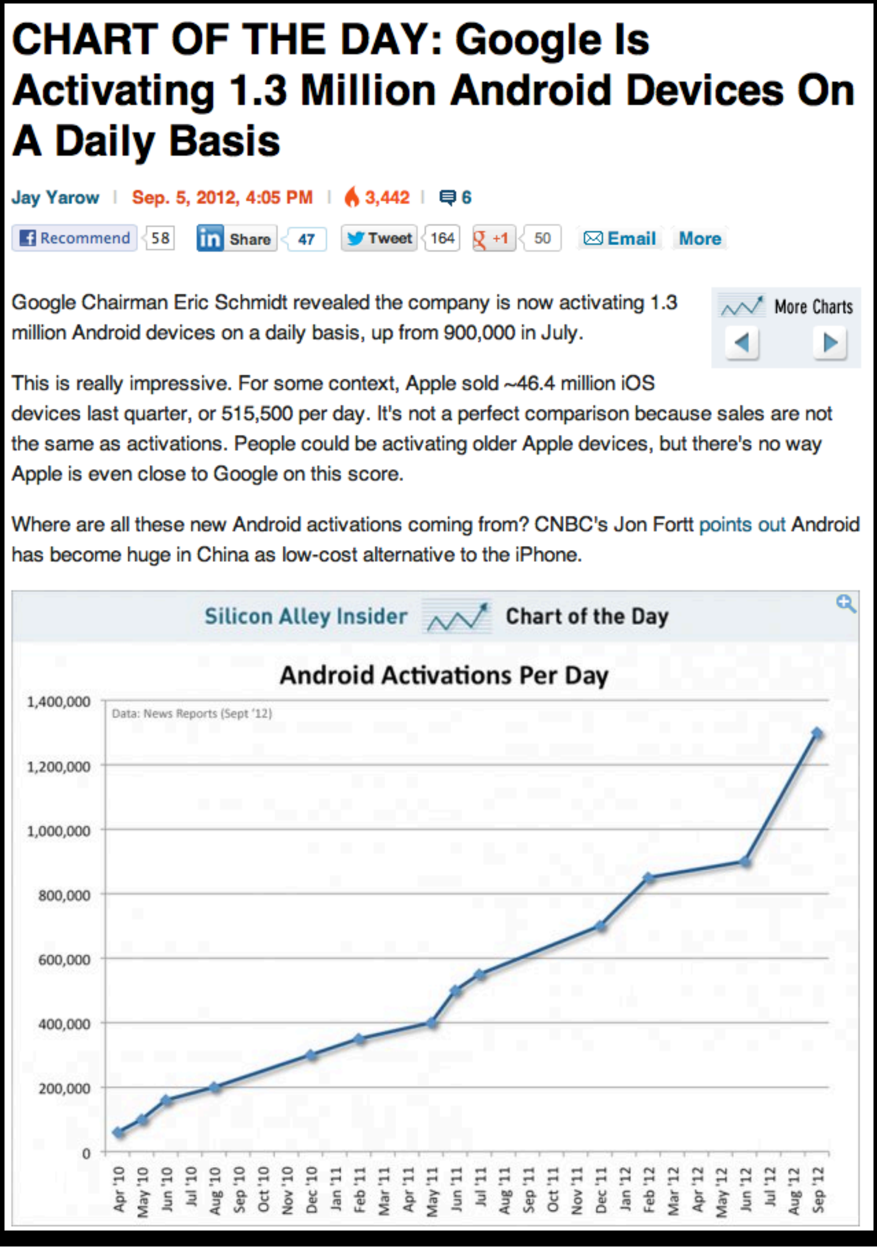


CHART OF THE DAY: Google Is Activating 1.3 Million Android Devices On A Daily Basis

Jay Yarow | Sep. 5, 2012, 4:05 PM | 3,442 | 6

Google Chairman Eric Schmidt revealed the company is now activating 1.3 million Android devices on a daily basis, up from 900,000 in July.

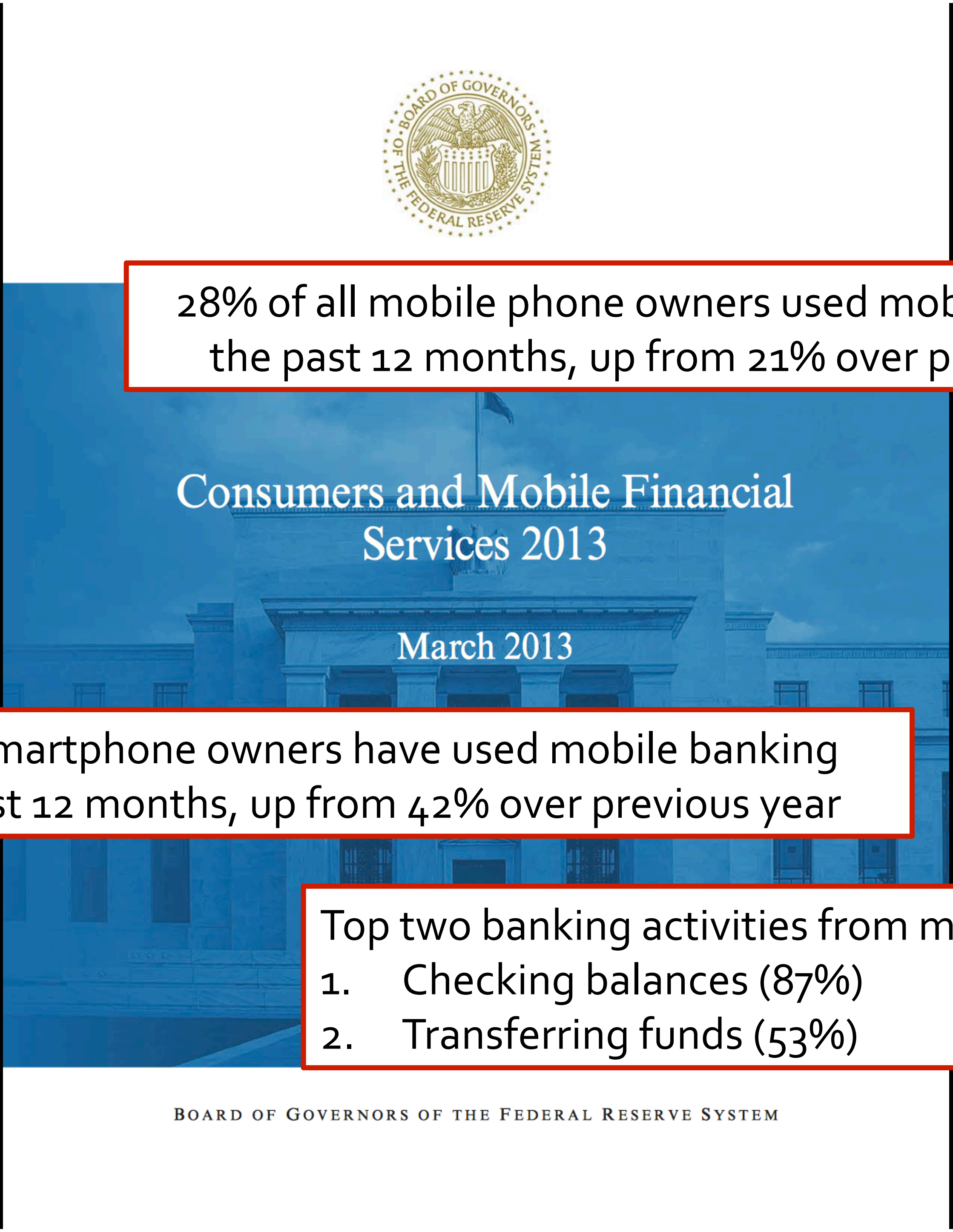
This is really impressive. For some context, Apple sold ~46.4 million iOS devices last quarter, or 515,500 per day. It's not a perfect comparison because sales are not the same as activations. People could be activating older Apple devices, but there's no way Apple is even close to Google on this score.

Where are all these new Android activations coming from? CNBC's Jon Fortt points out Android has become huge in China as low-cost alternative to the iPhone.

1,500,000 per day as of 16 APR 13.

But what about user behavior?

http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf



Consumers and Mobile Financial Services 2013

March 2013

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

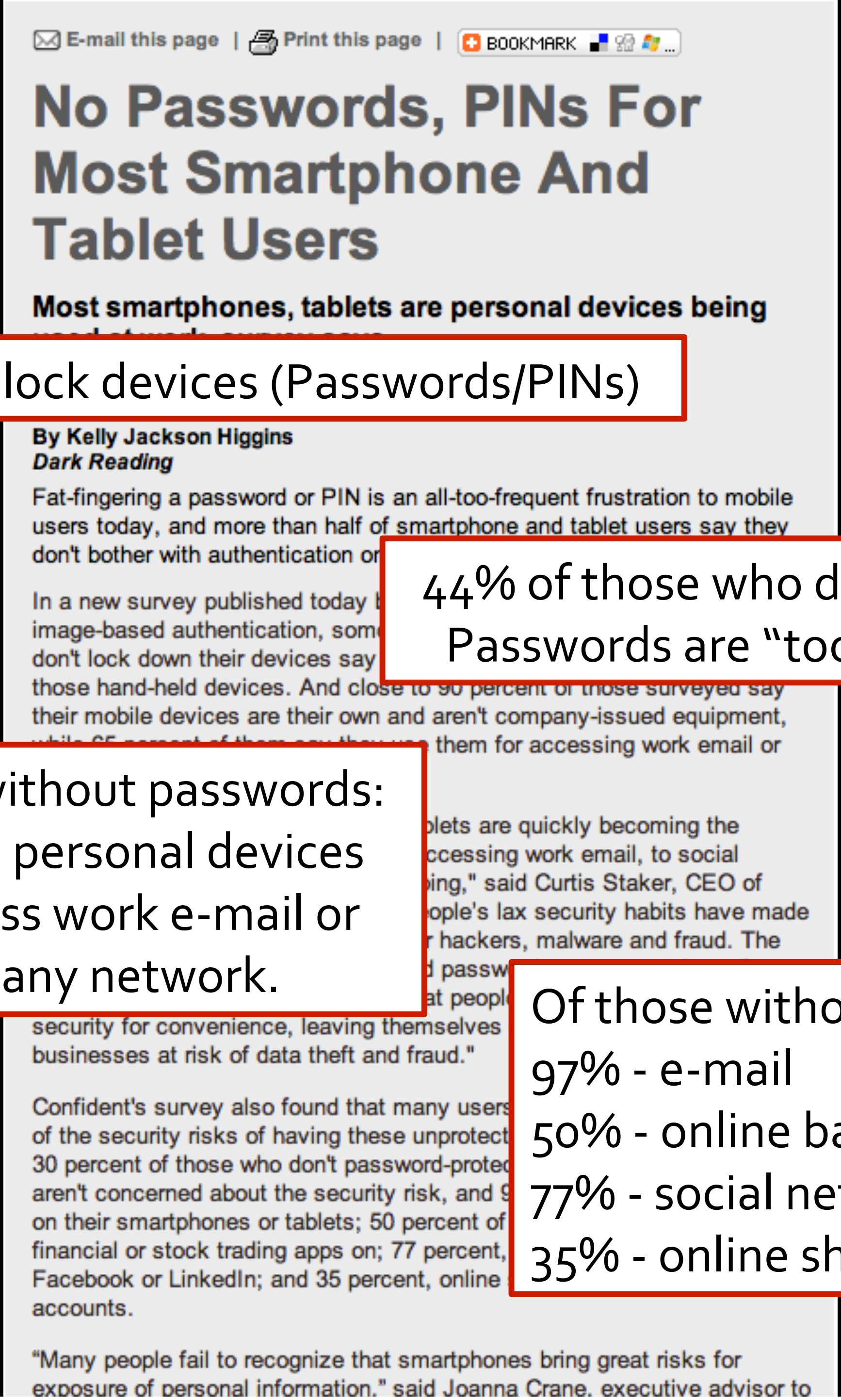
28% of all mobile phone owners used mobile banking in the past 12 months, up from 21% over previous year

48% of smartphone owners have used mobile banking in the past 12 months, up from 42% over previous year

Top two banking activities from mobile phones:

1. Checking balances (87%)
2. Transferring funds (53%)

http://www.darkreading.com/insider-threat/167801100/security/news/231602443/no-passwords-pins-for-most-smartphone-and-tablet-users.html



E-mail this page | Print this page | BOOKMARK

No Passwords, PINs For Most Smartphone And Tablet Users

Most smartphones, tablets are personal devices being

By Kelly Jackson Higgins
Dark Reading

Fat-fingering a password or PIN is an all-too-frequent frustration to mobile users today, and more than half of smartphone and tablet users say they don't bother with authentication or

In a new survey published today b
image-based authentication, som
don't lock down their devices say
those hand-held devices. And close to 90 percent of those surveyed say their mobile devices are their own and aren't company-issued equipment, while 65 percent of them say they use them for accessing work email or

blets are quickly becoming the
ccessing work email, to social
ing," said Curtis Staker, CEO of
ople's lax security habits have made
r hackers, malware and fraud. The
d passw
at peopl
security for convenience, leaving themselves
businesses at risk of data theft and fraud."

Confident's survey also found that many users
of the security risks of having these unprotect
30 percent of those who don't password-protec
aren't concerned about the security risk, and 9
on their smartphones or tablets; 50 percent of
financial or stock trading apps on; 77 percent,
Facebook or LinkedIn; and 35 percent, online
accounts.

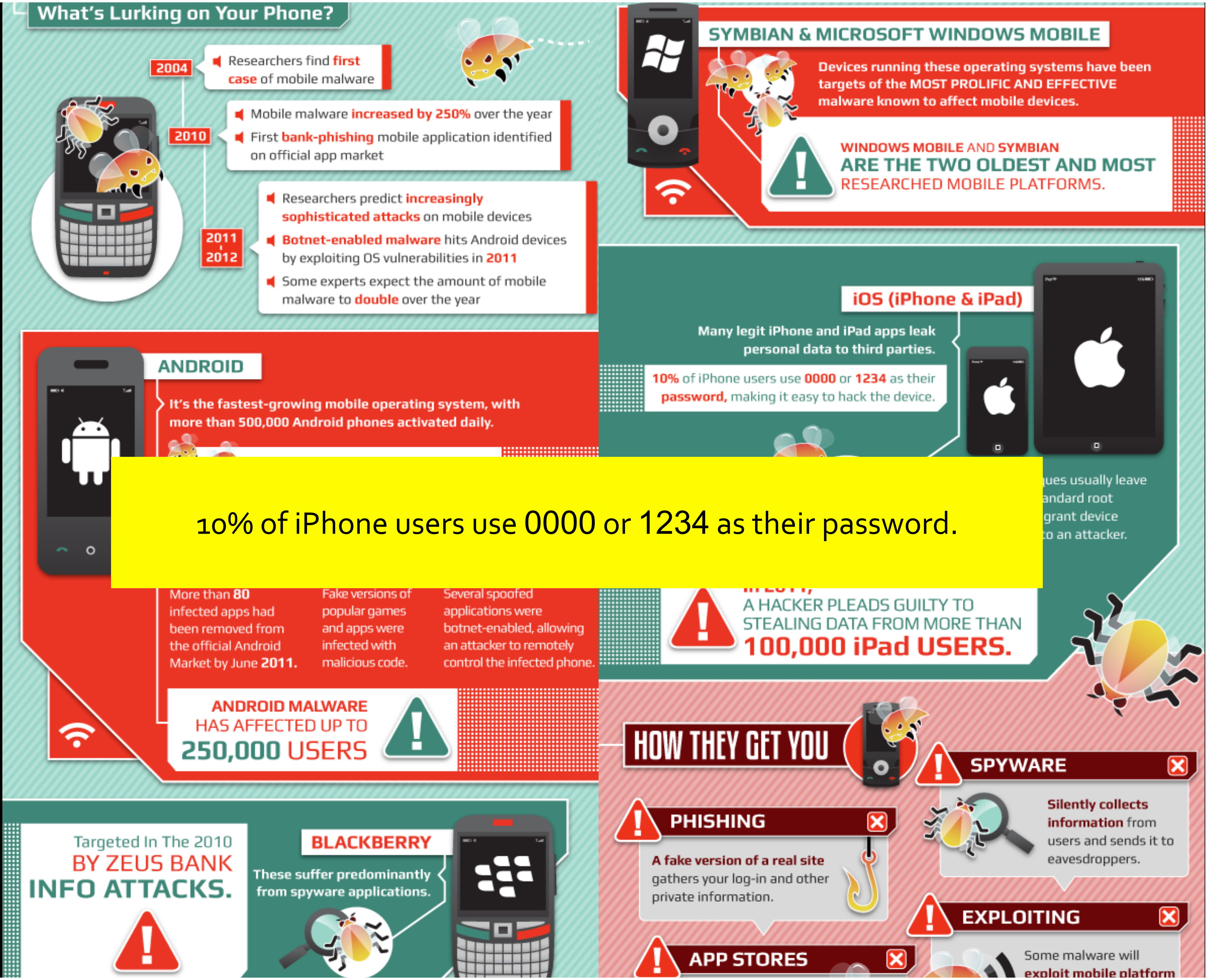
"Many people fail to recognize that smartphones bring great risks for exposure of personal information," said Joanna Crane, executive advisor to

50+% don't lock devices (Passwords/PINs)

44% of those who don't lock devices:
Passwords are "too cumbersome."

Of those without passwords:
~90% use personal devices
65% access work e-mail or company network.

Of those without passwords:
97% - e-mail
50% - online banking
77% - social networking
35% - online shopping



What's Lurking on Your Phone?

2004 – Researchers find **first case** of mobile malware

2010 – Mobile malware **increased by 250%** over the year

First **bank-phishing** mobile application identified on official app market

2011 2012 – Researchers predict **increasingly sophisticated attacks** on mobile devices

Botnet-enabled malware hits Android devices by exploiting OS vulnerabilities in **2011**

Some experts expect the amount of mobile malware to **double** over the year

SYMBIAN & MICROSOFT WINDOWS MOBILE

Devices running these operating systems have been targets of the MOST PROLIFIC AND EFFECTIVE malware known to affect mobile devices.

WINDOWS MOBILE AND SYMBIAN ARE THE TWO OLDEST AND MOST RESEARCHED MOBILE PLATFORMS.

ANDROID

It's the fastest-growing mobile operating system, with more than 500,000 Android phones activated daily.

More than **80** infected apps had been removed from the official Android Market by June **2011.**

Fake versions of popular games and apps were infected with malicious code.

Several spoofed applications were botnet-enabled, allowing an attacker to remotely control the infected phone.

ANDROID MALWARE HAS AFFECTED UP TO 250,000 USERS

iOS (iPhone & iPad)

Many legit iPhone and iPad apps leak personal data to third parties.

10% of iPhone users use **0000** or **1234** as their **password,** making it easy to hack the device.

ues usually leave
andard root
grant device
to an attacker.

A HACKER PLEADS GUILTY TO STEALING DATA FROM MORE THAN **100,000 iPad USERS.**

Targeted In The 2010 BY ZEUS BANK INFO ATTACKS.

BLACKBERRY

These suffer predominantly from spyware applications.

HOW THEY GET YOU

SPYWARE – **Silently collects information** from users and sends it to eavesdroppers.

PHISHING – **A fake version of a real site** gathers your log-in and other private information.

EXPLOITING – Some malware will exploit mobile platform

APP STORES

10% of iPhone users use 0000 or 1234 as their password.

http://mashable.com/2011/08/12/mobile-malware/

Bullguard

But that was 2011 (ages ago).

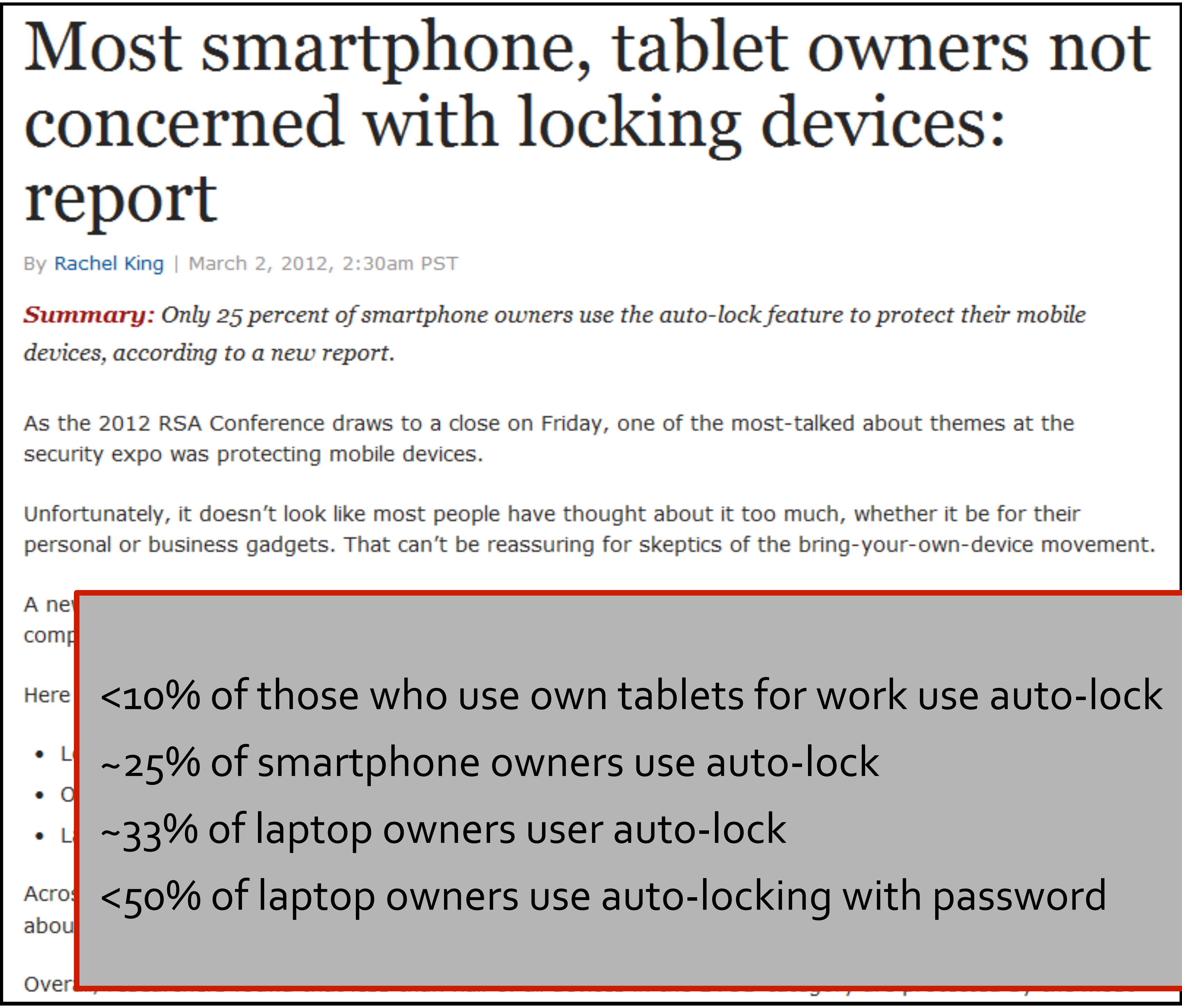
Surely we've gotten better, right?

As of 2013:

~50% of users do not use passwords to secure their mobile devices

Sources: Consumer Reports, Symantec

http://msisac.cisecurity.org/resources/reports/documents/b-norton-report-2013.pdf http://www.zdnet.com/blog/btl/most-smartphone-tablet-owners-not-concerned-with-locking-devices-report/70672



Most smartphone, tablet owners not concerned with locking devices: report

By Rachel King | March 2, 2012, 2:30am PST

Summary: *Only 25 percent of smartphone owners use the auto-lock feature to protect their mobile devices, according to a new report.*

As the 2012 RSA Conference draws to a close on Friday, one of the most-talked about themes at the security expo was protecting mobile devices.

Unfortunately, it doesn't look like most people have thought about it too much, whether it be for their personal or business gadgets. That can't be reassuring for skeptics of the bring-your-own-device movement.

A ne
comp

Here

- L
- O
- L

Acro
abou

Over

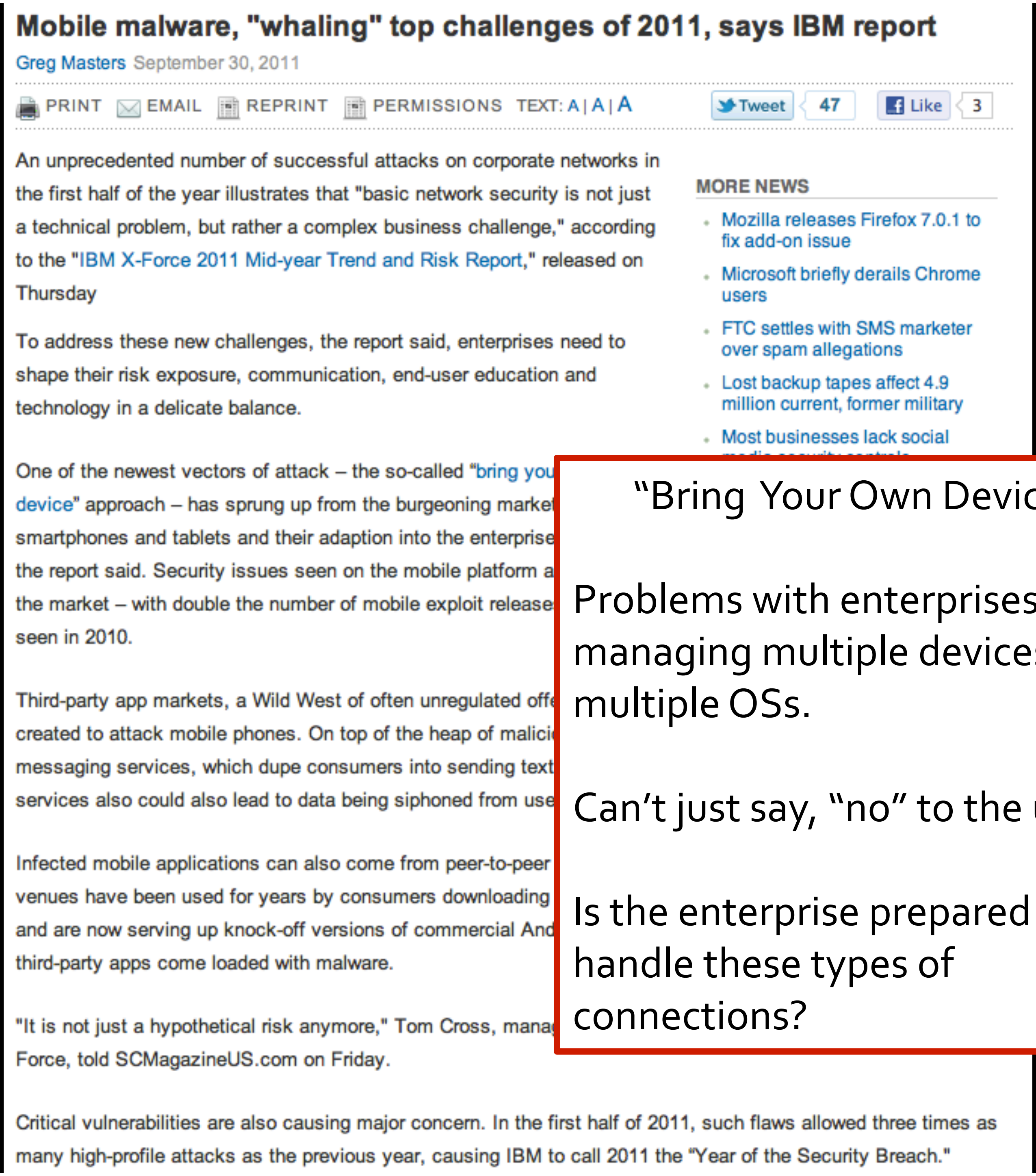
<10% of those who use own tablets for work use auto-lock

~25% of smartphone owners use auto-lock

~33% of laptop owners user auto-lock

<50% of laptop owners use auto-locking with password

http://www.scmagazineus.com/mobile-malware-whaling-top-challenges-of-2011-says-ibm-report/article/213219/



Mobile malware, "whaling" top challenges of 2011, says IBM report

Greg Masters September 30, 2011

An unprecedented number of successful attacks on corporate networks in the first half of the year illustrates that "basic network security is not just a technical problem, but rather a complex business challenge," according to the "IBM X-Force 2011 Mid-year Trend and Risk Report," released on Thursday

To address these new challenges, the report said, enterprises need to shape their risk exposure, communication, end-user education and technology in a delicate balance.

One of the newest vectors of attack – the so-called "bring you device" approach – has sprung up from the burgeoning market smartphones and tablets and their adaption into the enterprise the report said. Security issues seen on the mobile platform a the market – with double the number of mobile exploit release seen in 2010.

Third-party app markets, a Wild West of often unregulated offe created to attack mobile phones. On top of the heap of malicio messaging services, which dupe consumers into sending text services also could also lead to data being siphoned from use

Infected mobile applications can also come from peer-to-peer venues have been used for years by consumers downloading and are now serving up knock-off versions of commercial And third-party apps come loaded with malware.

"It is not just a hypothetical risk anymore," Tom Cross, mana Force, told SCMagazineUS.com on Friday.

Critical vulnerabilities are also causing major concern. In the first half of 2011, such flaws allowed three times as many high-profile attacks as the previous year, causing IBM to call 2011 the "Year of the Security Breach."

MORE NEWS

- Mozilla releases Firefox 7.0.1 to fix add-on issue
- Microsoft briefly derails Chrome users
- FTC settles with SMS marketer over spam allegations
- Lost backup tapes affect 4.9 million current, former military
- Most businesses lack social

“Bring Your Own Device”

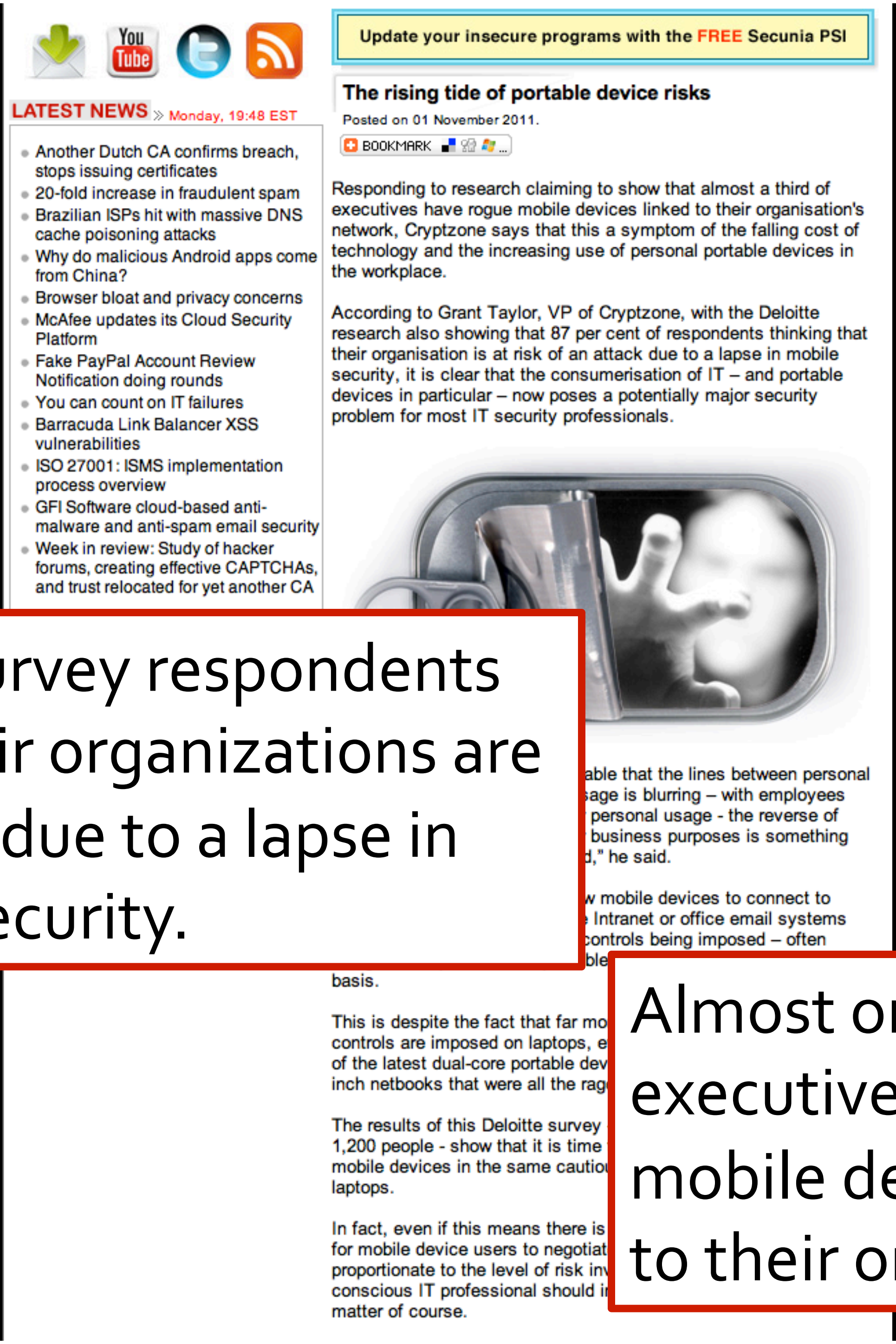
Problems with enterprises managing multiple devices with multiple OSs.

Can’t just say, “no” to the users.

Is the enterprise prepared to handle these types of connections?

Do you think enterprises are ready
for the onslaught of mobile devices?

http://www.net-security.org/secworld.php?id=11869



LATEST NEWS » Monday, 19:48 EST

- Another Dutch CA confirms breach, stops issuing certificates
- 20-fold increase in fraudulent spam
- Brazilian ISPs hit with massive DNS cache poisoning attacks
- Why do malicious Android apps come from China?
- Browser bloat and privacy concerns
- McAfee updates its Cloud Security Platform
- Fake PayPal Account Review Notification doing rounds
- You can count on IT failures
- Barracuda Link Balancer XSS vulnerabilities
- ISO 27001: ISMS implementation process overview
- GFI Software cloud-based anti-malware and anti-spam email security
- Week in review: Study of hacker forums, creating effective CAPTCHAs, and trust relocated for yet another CA

The rising tide of portable device risks

Posted on 01 November 2011.

Responding to research claiming to show that almost a third of executives have rogue mobile devices linked to their organisation's network, Cryptzone says that this a symptom of the falling cost of technology and the increasing use of personal portable devices in the workplace.

According to Grant Taylor, VP of Cryptzone, with the Deloitte research also showing that 87 per cent of respondents thinking that their organisation is at risk of an attack due to a lapse in mobile security, it is clear that the consumerisation of IT – and portable devices in particular – now poses a potentially major security problem for most IT security professionals.

able that the lines between personal
sage is blurring – with employees
personal usage - the reverse of
business purposes is something
d," he said.

w mobile devices to connect to
Intranet or office email systems
controls being imposed – often
ble
basis.

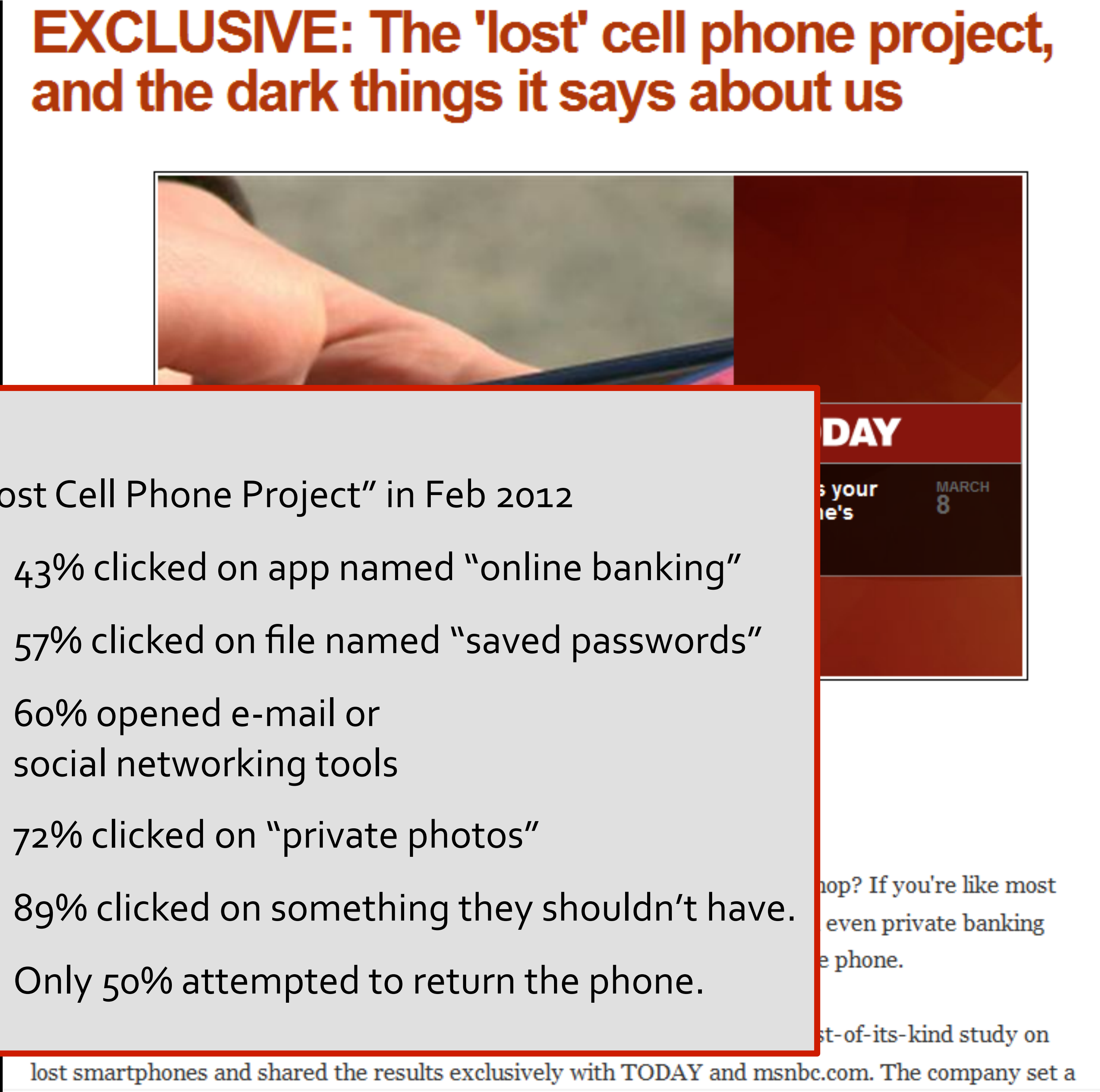
This is despite the fact that far mo
controls are imposed on laptops, e
of the latest dual-core portable dev
inch netbooks that were all the rag

The results of this Deloitte survey
1,200 people - show that it is time
mobile devices in the same cautio
laptops.

In fact, even if this means there is
for mobile device users to negotiat
proportionate to the level of risk in
conscious IT professional should i
matter of course.

87% of survey respondents think their organizations are at risk to due to a lapse in mobile security.

Almost one-third of executives have rogue mobile devices linked to their org's networks.



EXCLUSIVE: The 'lost' cell phone project, and the dark things it says about us

hop? If you're like most
even private banking
e phone.

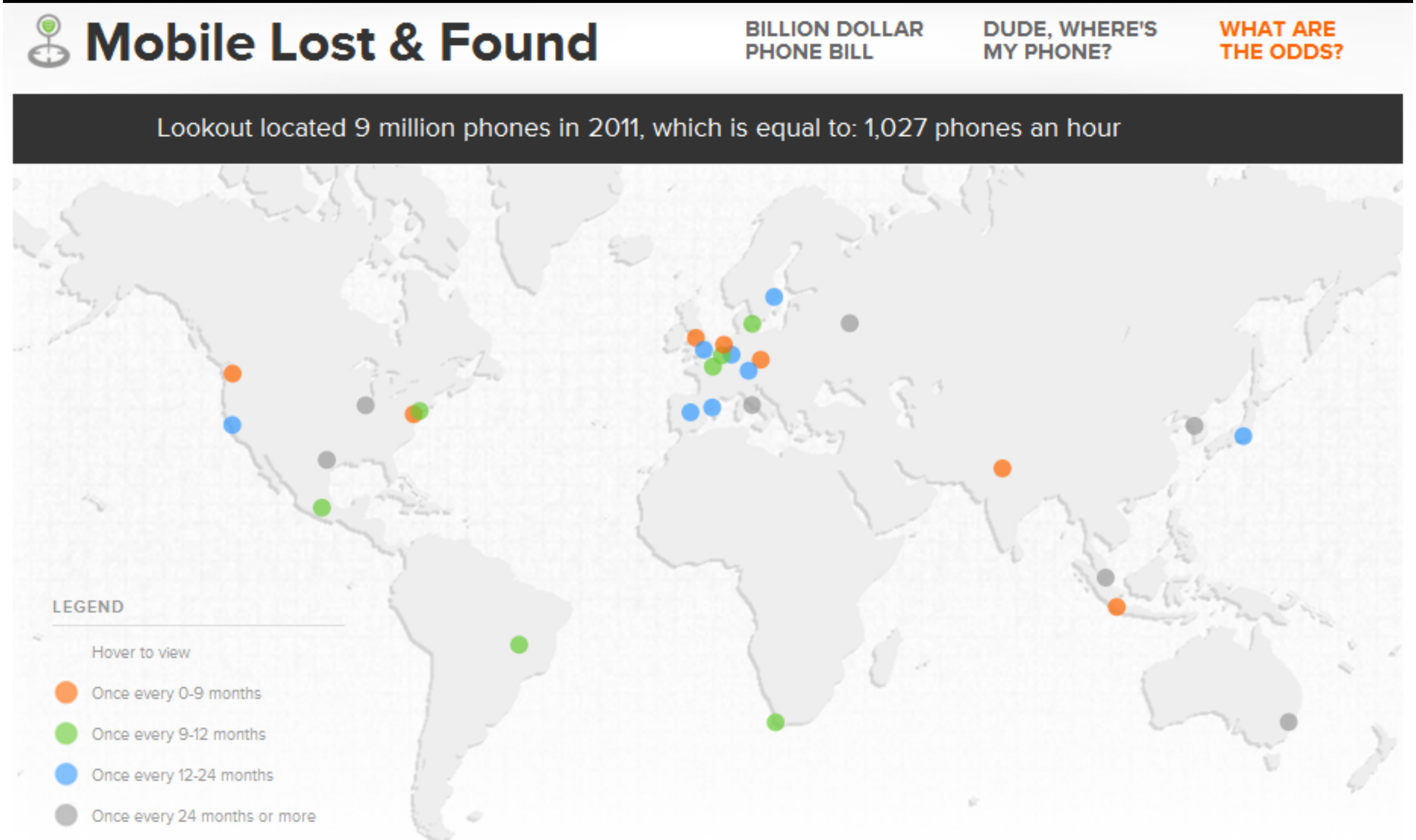
st-of-its-kind study on
lost smartphones and shared the results exclusively with TODAY and msnbc.com. The company set a

"Lost Cell Phone Project" in Feb 2012

- 43% clicked on app named "online banking"
- 57% clicked on file named "saved passwords"
- 60% opened e-mail or social networking tools
- 72% clicked on "private photos"
- 89% clicked on something they shouldn't have.
- Only 50% attempted to return the phone.

http://digitallife.today.msnbc.msn.com/_news/2012/03/08/10595092-exclusive-the-lost-cell-phone-project-and-the-dark-things-it-says-about-us

So what are the odds of losing a phone?



Mobile Lost & Found

BILLION DOLLAR PHONE BILL

DUDE, WHERE'S MY PHONE?

WHAT ARE THE ODDS?

Lookout located 9 million phones in 2011, which is equal to: 1,027 phones an hour

LEGEND

Hover to view

🟠 Once every 0-9 months

🟢 Once every 9-12 months

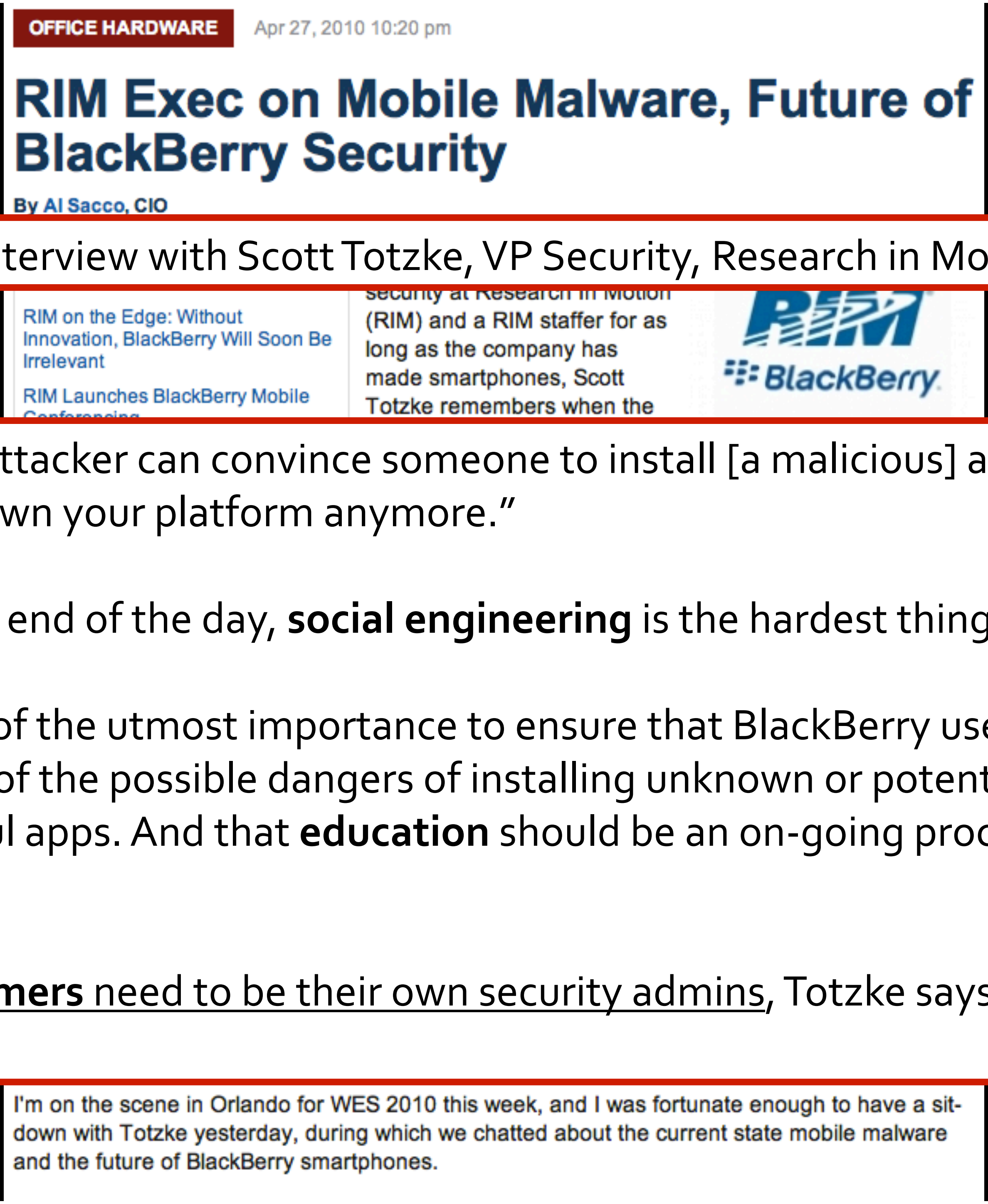
🔵 Once every 12-24 months

● Once every 24 months or more

https://www.mylookout.com/resources/reports/mobile-lost-and-found/what-are-the-odds

Is there a fix?

http://www.pcworld.com/businesscenter/article/195115/rim_exec_on_mobile_malware_future_of_blackberry_security.html



OFFICE HARDWARE Apr 27, 2010 10:20 pm

RIM Exec on Mobile Malware, Future of BlackBerry Security

By Al Sacco, CIO

Interview with Scott Totzke, VP Security, Research in Motion

RIM on the Edge: Without Innovation, BlackBerry Will Soon Be Irrelevant

RIM Launches BlackBerry Mobile Conferencing

security at Research in Motion (RIM) and a RIM staffer for as long as the company has made smartphones, Scott Totzke remembers when the

“If an attacker can convince someone to install [a malicious] app, you don't own your platform anymore.”

"At the end of the day, **social engineering** is the hardest thing to fix.“

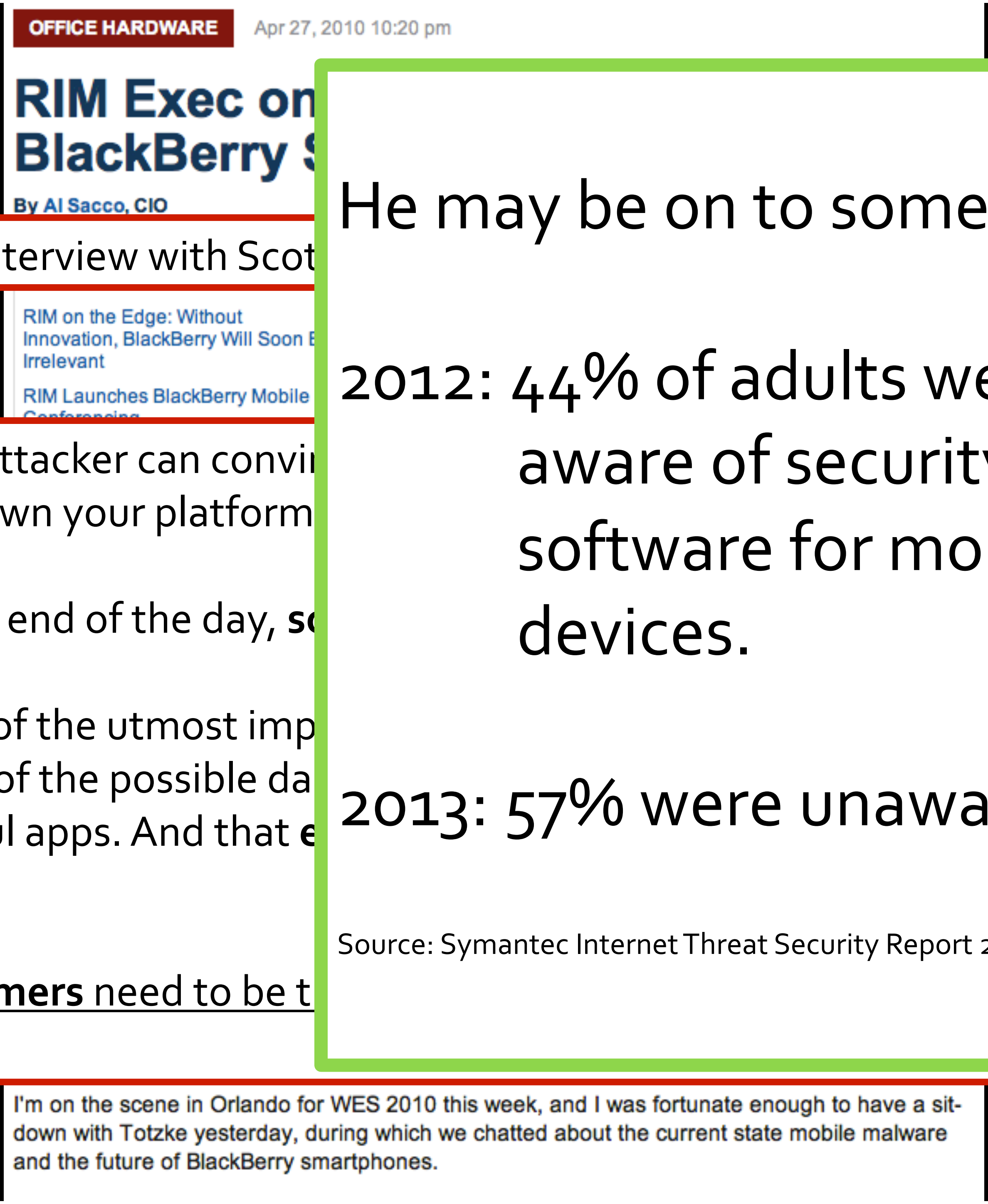
So it's of the utmost importance to ensure that BlackBerry users are aware of the possible dangers of installing unknown or potentially harmful apps. And that **education** should be an on-going process, he says.

<u>**Consumers** need to be their own security admins</u>, Totzke says.

I'm on the scene in Orlando for WES 2010 this week, and I was fortunate enough to have a sit-down with Totzke yesterday, during which we chatted about the current state mobile malware and the future of BlackBerry smartphones.

Education…consumers…

http://www.pcworld.com/businesscenter/article/195115/rim_exec_on_mobile_malware_future_of_blackberry_security.html



OFFICE HARDWARE Apr 27, 2010 10:20 pm

RIM Exec on
BlackBerry S

By Al Sacco, CIO

RIM on the Edge: Without Innovation, BlackBerry Will Soon B
Irrelevant

RIM Launches BlackBerry Mobile
Conferencing

I'm on the scene in Orlando for WES 2010 this week, and I was fortunate enough to have a sit-down with Totzke yesterday, during which we chatted about the current state mobile malware and the future of BlackBerry smartphones.

Interview with Scot

“If an attacker can convi
don't own your platform

"At the end of the day, **s**

So it's of the utmost imp
aware of the possible da
harmful apps. And that **e**
says.

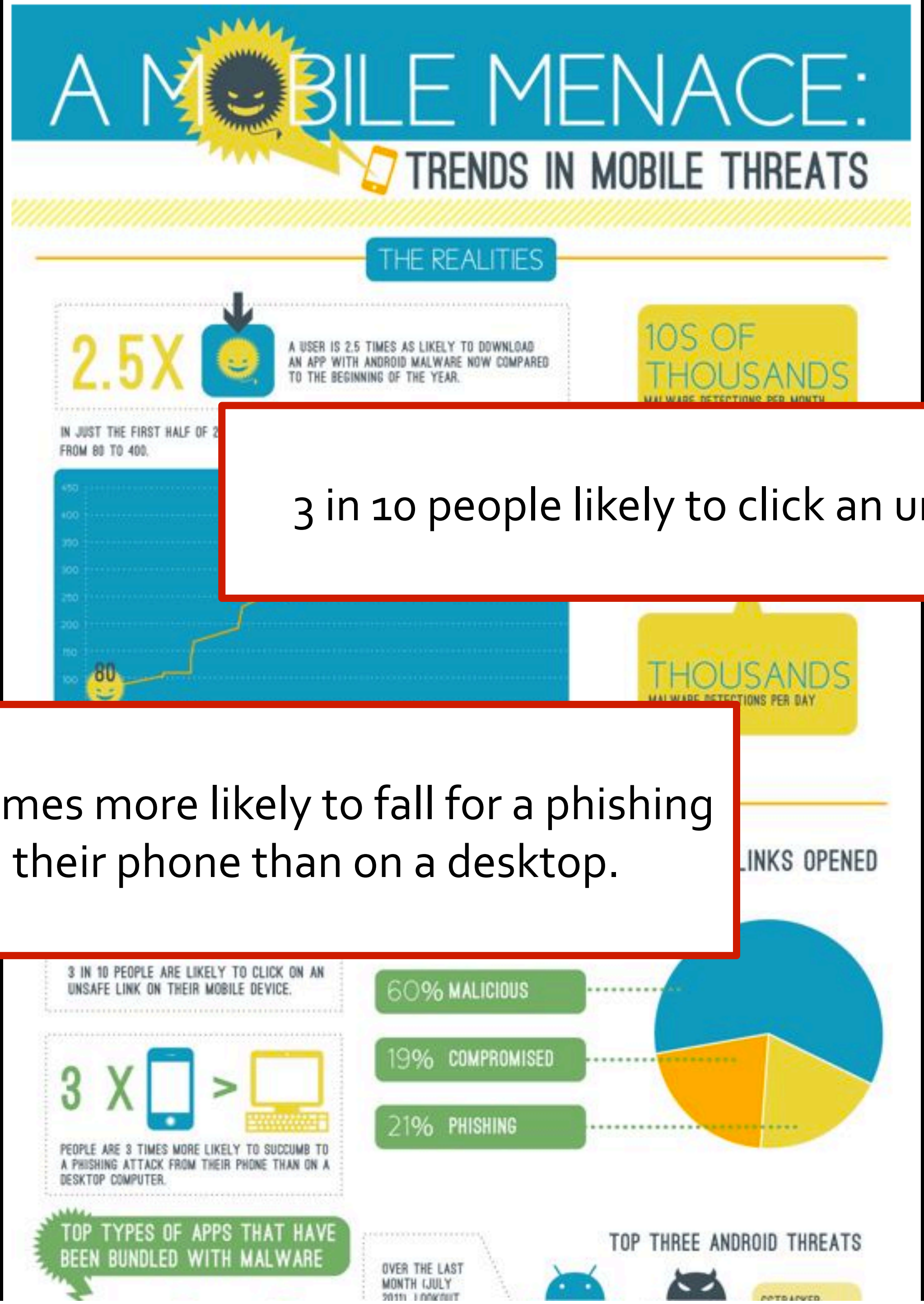
<u>**Consumers** need to be t</u>

He may be on to something:

2012: 44% of adults were not aware of security software for mobile devices.

2013: 57% were unaware.

Source: Symantec Internet Threat Security Report 2014



A USER IS 2.5 TIMES AS LIKELY TO DOWNLOAD AN APP WITH ANDROID MALWARE NOW COMPARED TO THE BEGINNING OF THE YEAR.

IN JUST THE FIRST HALF OF 2

FROM 80 TO 400.

3 IN 10 PEOPLE ARE LIKELY TO CLICK ON AN UNSAFE LINK ON THEIR MOBILE DEVICE.

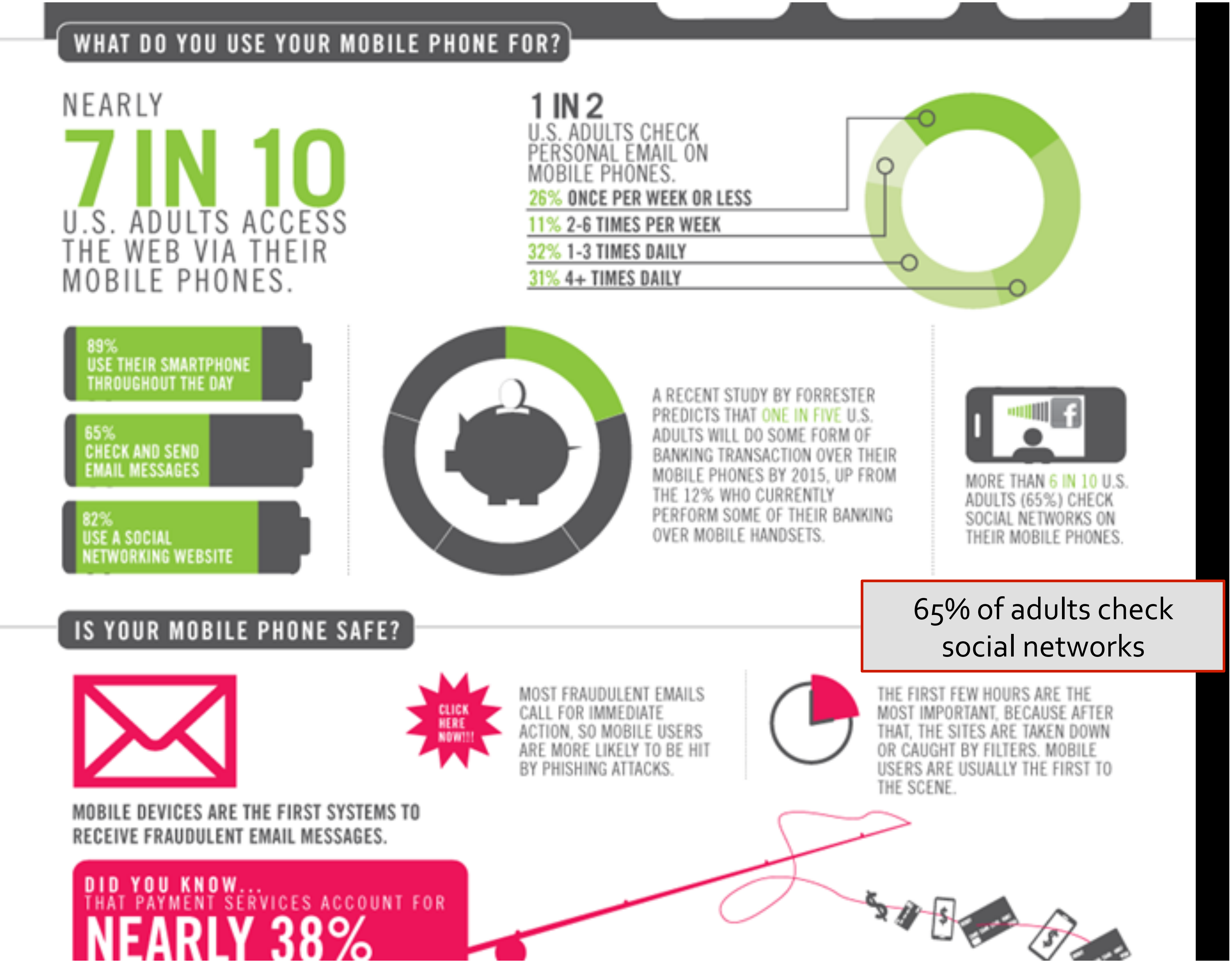
PEOPLE ARE 3 TIMES MORE LIKELY TO SUCCUMB TO A PHISHING ATTACK FROM THEIR PHONE THAN ON A DESKTOP COMPUTER.

OVER THE LAST MONTH (JULY 2011) LOOKOUT

3 in 10 people likely to click an unsafe link.

People are 3 times more likely to fall for a phishing attack on their phone than on a desktop.

http://www.unplggd.com/unplggd/safety-security/does-your-smartphone-need-antivirus-protection-156222



WHAT DO YOU USE YOUR MOBILE PHONE FOR?

NEARLY **7 IN 10** U.S. ADULTS ACCESS THE WEB VIA THEIR MOBILE PHONES.

1 IN 2 U.S. ADULTS CHECK PERSONAL EMAIL ON MOBILE PHONES.

- 26% ONCE PER WEEK OR LESS
- 11% 2-6 TIMES PER WEEK
- 32% 1-3 TIMES DAILY
- 31% 4+ TIMES DAILY

89% USE THEIR SMARTPHONE THROUGHOUT THE DAY

65% CHECK AND SEND EMAIL MESSAGES

82% USE A SOCIAL NETWORKING WEBSITE

A RECENT STUDY BY FORRESTER PREDICTS THAT ONE IN FIVE U.S. ADULTS WILL DO SOME FORM OF BANKING TRANSACTION OVER THEIR MOBILE PHONES BY 2015, UP FROM THE 12% WHO CURRENTLY PERFORM SOME OF THEIR BANKING OVER MOBILE HANDSETS.

MORE THAN 6 IN 10 U.S. ADULTS (65%) CHECK SOCIAL NETWORKS ON THEIR MOBILE PHONES.

IS YOUR MOBILE PHONE SAFE?

MOBILE DEVICES ARE THE FIRST SYSTEMS TO RECEIVE FRAUDULENT EMAIL MESSAGES.

MOST FRAUDULENT EMAILS CALL FOR IMMEDIATE ACTION, SO MOBILE USERS ARE MORE LIKELY TO BE HIT BY PHISHING ATTACKS.

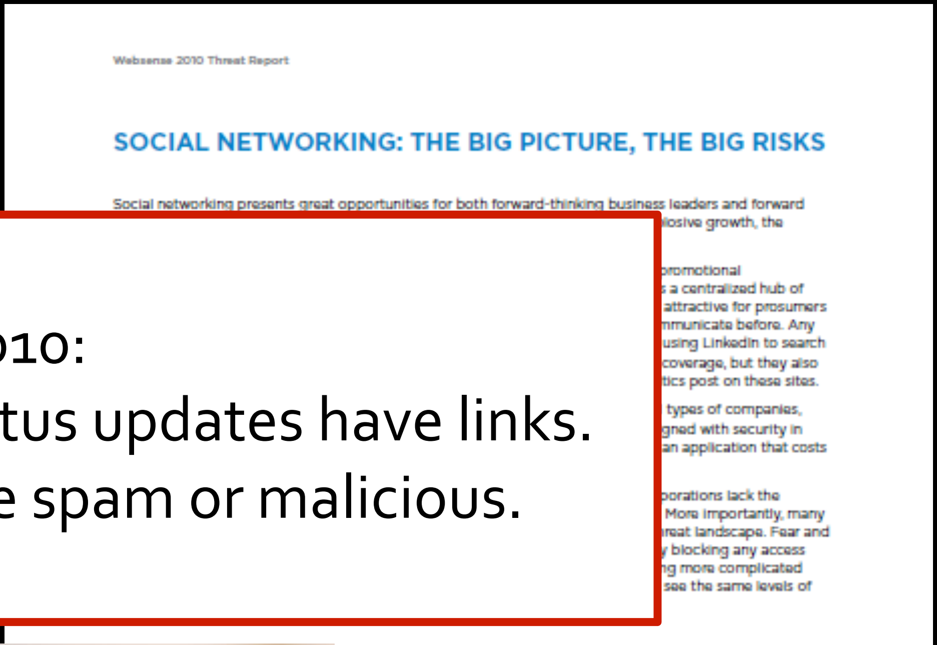
THE FIRST FEW HOURS ARE THE MOST IMPORTANT, BECAUSE AFTER THAT, THE SITES ARE TAKEN DOWN OR CAUGHT BY FILTERS. MOBILE USERS ARE USUALLY THE FIRST TO THE SCENE.

DID YOU KNOW... THAT PAYMENT SERVICES ACCOUNT FOR NEARLY 38%

65% of adults check social networks

https://www.mylookout.com/_downloads/infographics/Lookout_what_is_phishing.png

https://www.websense.com/assets/reports/report-websense-2010-threat-report-en.pdf
http://www.lifed.com/15-must-have-free-android-apps-for-2011



Websense 2010 Threat Report

SOCIAL NETWORKING: THE BIG PICTURE, THE BIG RISKS

Social networking presents great opportunities for both forward-thinking business leaders and forward
losive growth, the

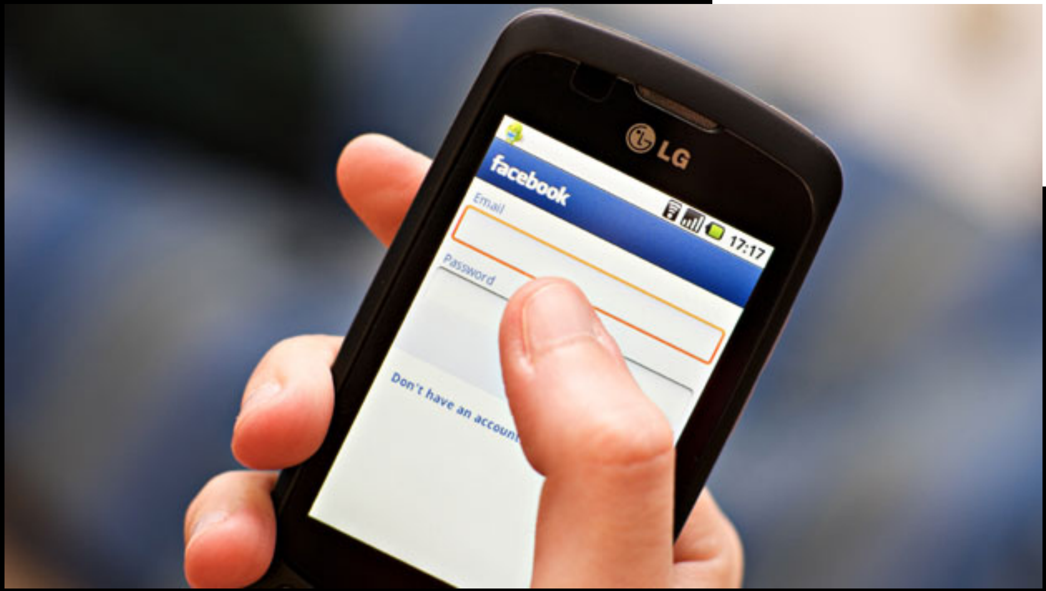
promotional
s a centralized hub of
attractive for prosumers
mmunicate before. Any
using LinkedIn to search
coverage, but they also
tics post on these sites.

types of companies,
gned with security in
an application that costs

porations lack the
More importantly, many
reat landscape. Fear and
y blocking any access
ng more complicated
see the same levels of

40% of all Facebook status updates have links and 10% of those links are either spam or malicious.

In 2010:
40% of all Facebook status updates have links.
10% of those links are spam or malicious.



Likejacking

Using fake “Like” buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user’s newsfeed, spreading the attack.

Popular Attack Vectors

- SMS messages
- Infected applications
- Infected websites – click-thrus
- Intercepted Wi-Fi traffic

The Asian Influence

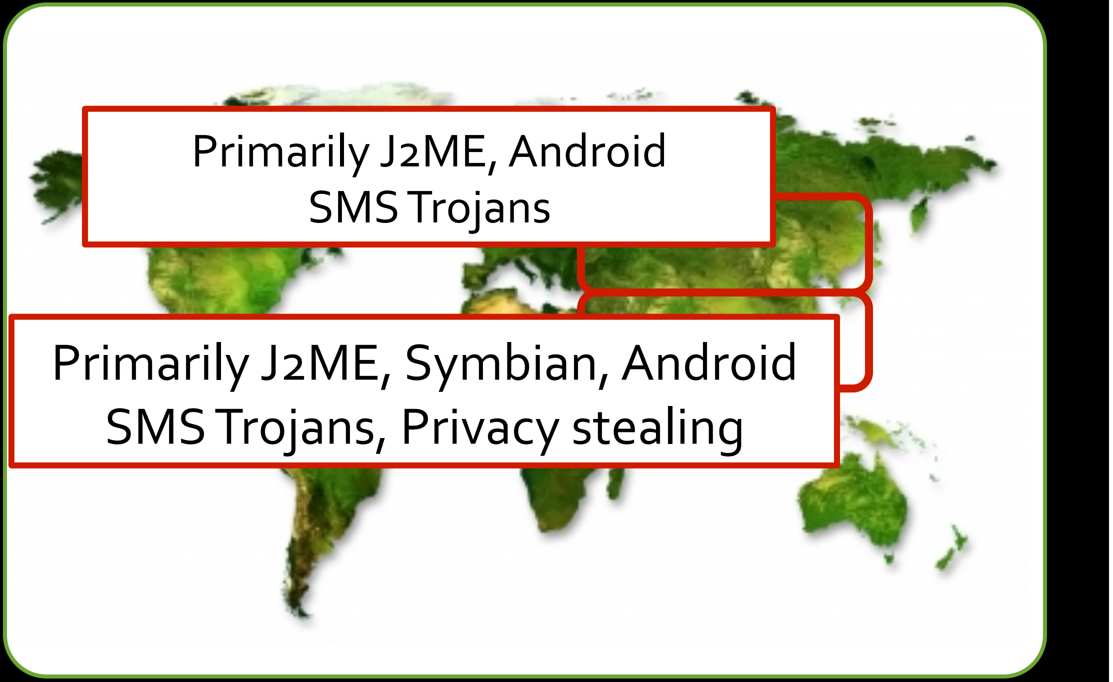
Based on attack vectors, re-used code, and other characteristics, malware is originating from:

- China
- Russia

The Asian Influence

Based on attack vectors, re-used code, and other characteristics, malware is originating from:

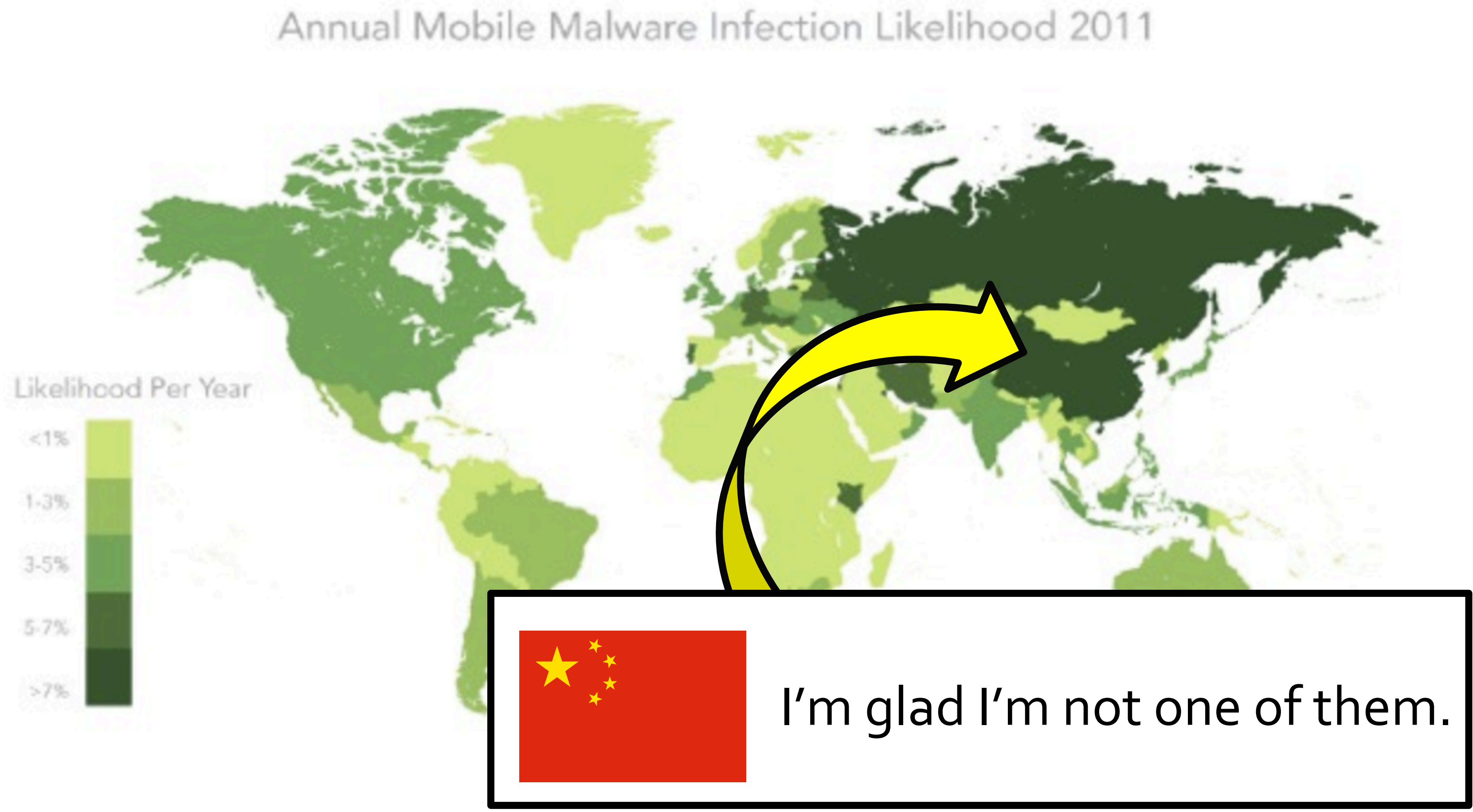
- China
- Russia



Primarily J2ME, Android SMS Trojans

Primarily J2ME, Symbian, Android SMS Trojans, Privacy stealing

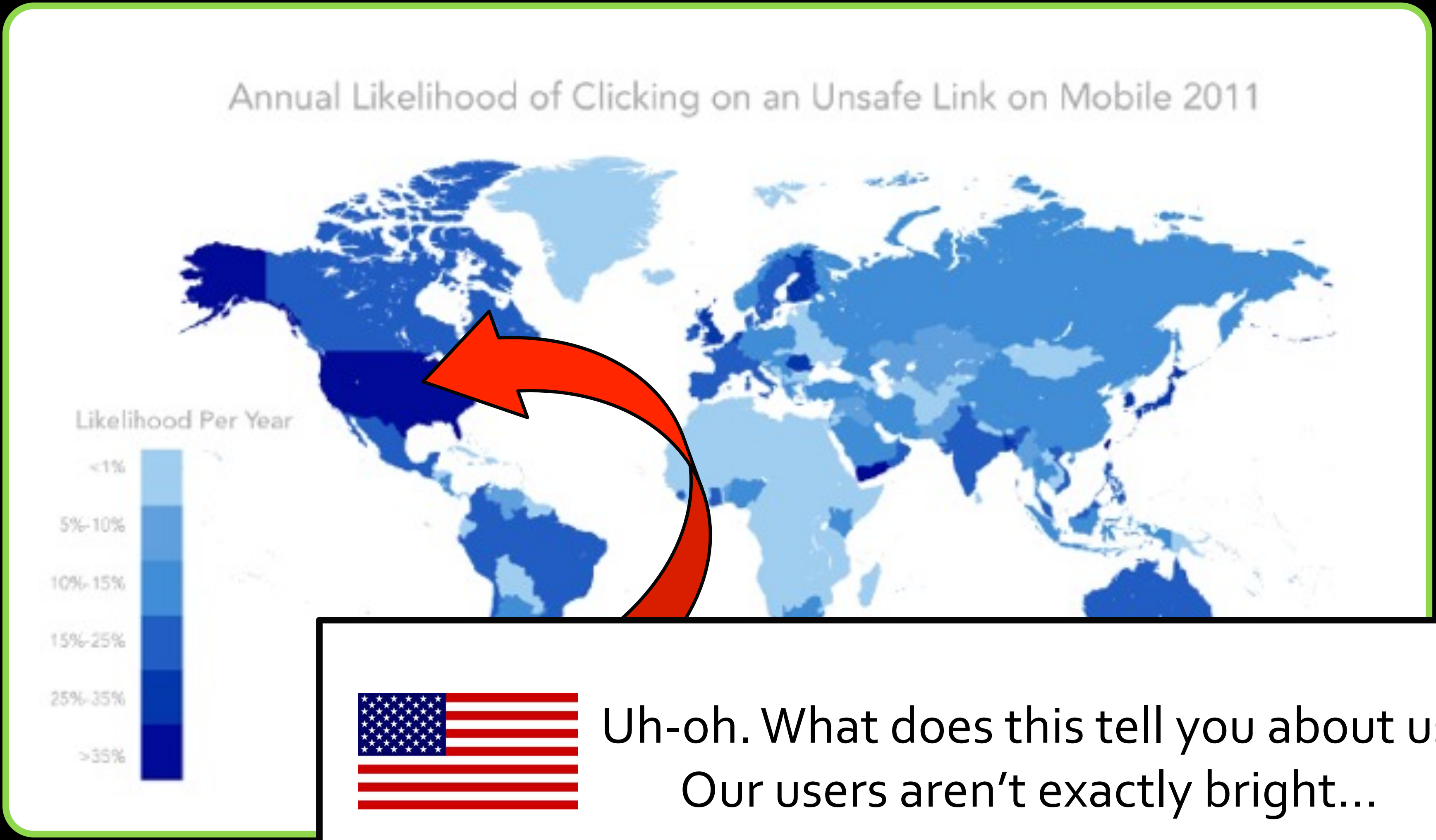
That was who makes it.
But who is likely to get bit?



Annual Mobile Malware Infection Likelihood 2011

I'm glad I'm not one of them.

http://www.readwriteweb.com/archives/6_mobile_malware_predictions_for_2012.php


Annual Likelihood of Clicking on an Unsafe Link on Mobile 2011
Likelihood Per Year
<1%
5%-10%
10%-15%
15%-25%
25%-35%
>35%

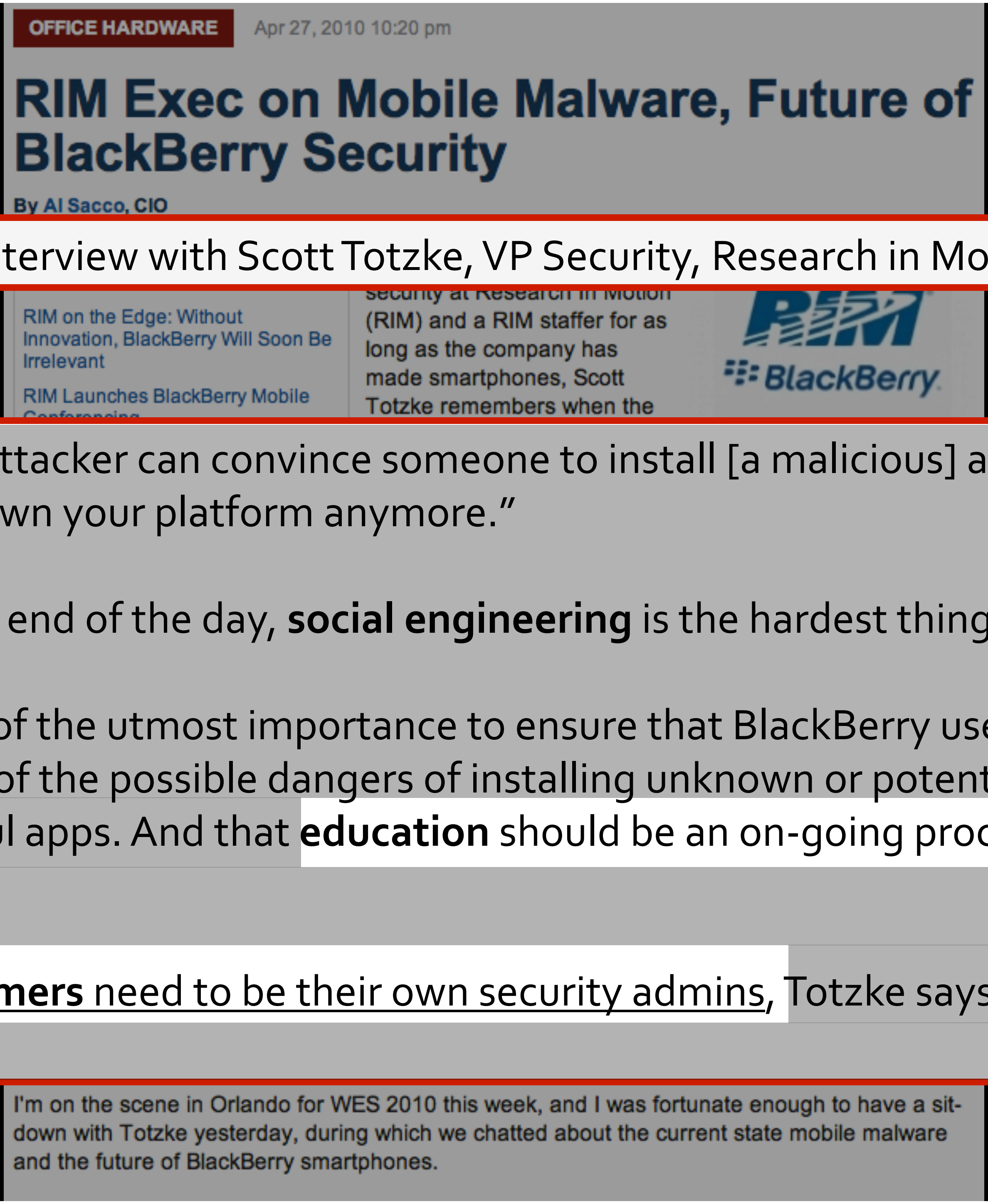
Uh-oh. What does this tell you about us?

Our users aren't exactly bright…

http://www.readwriteweb.com/archives/6_mobile_malware_predictions_for_2012.php

Remember…

http://www.pcworld.com/businesscenter/article/195115/rim_exec_on_mobile_malware_future_of_blackberry_security.html



OFFICE HARDWARE Apr 27, 2010 10:20 pm

RIM Exec on Mobile Malware, Future of BlackBerry Security

By Al Sacco, CIO

Interview with Scott Totzke, VP Security, Research in Motion

RIM on the Edge: Without Innovation, BlackBerry Will Soon Be Irrelevant

RIM Launches BlackBerry Mobile Conferencing

security at Research in Motion (RIM) and a RIM staffer for as long as the company has made smartphones, Scott Totzke remembers when the

“If an attacker can convince someone to install [a malicious] app, you don't own your platform anymore.”

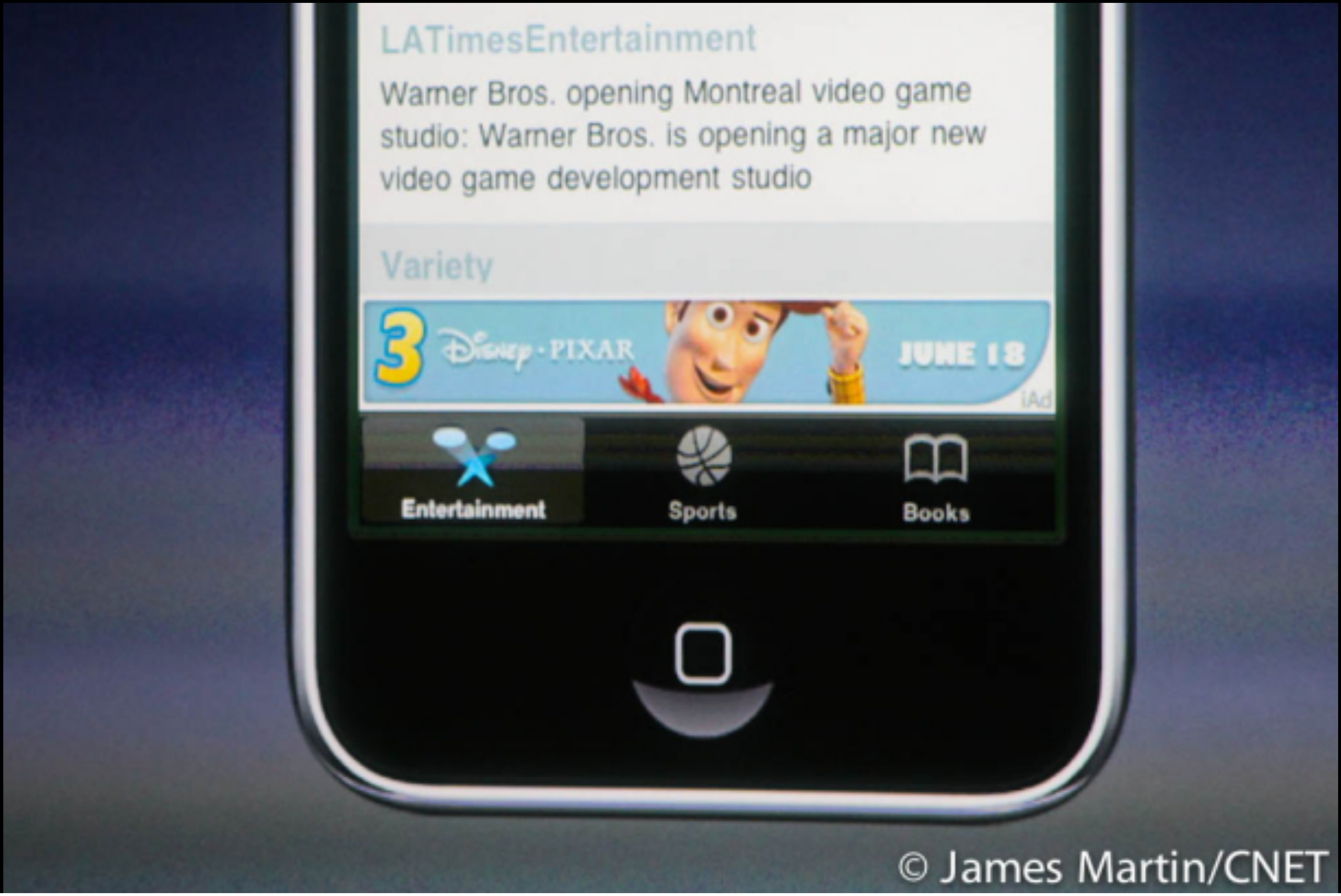
"At the end of the day, **social engineering** is the hardest thing to fix.“

So it's of the utmost importance to ensure that BlackBerry users are aware of the possible dangers of installing unknown or potentially harmful apps. And that **education** should be an on-going process, he says.

Consumers need to be their own security admins, Totzke says.

I'm on the scene in Orlando for WES 2010 this week, and I was fortunate enough to have a sit-down with Totzke yesterday, during which we chatted about the current state mobile malware and the future of BlackBerry smartphones.

Have you seen ads like this?

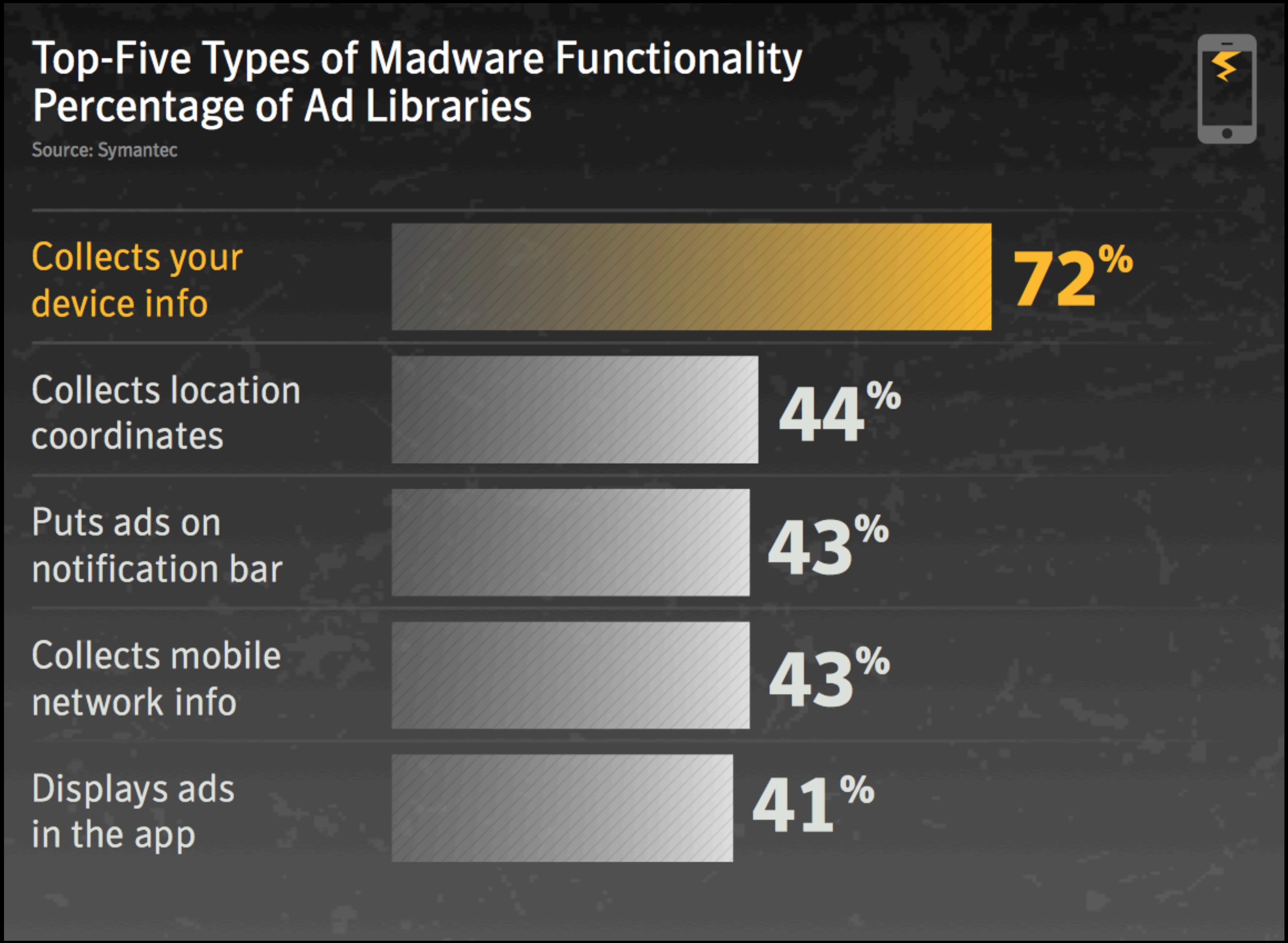


LATimesEntertainment

Warner Bros. opening Montreal video game studio: Warner Bros. is opening a major new video game development studio

© James Martin/CNET

Madware – Mobile Adware
How many times have you seen ads in free versions of apps?



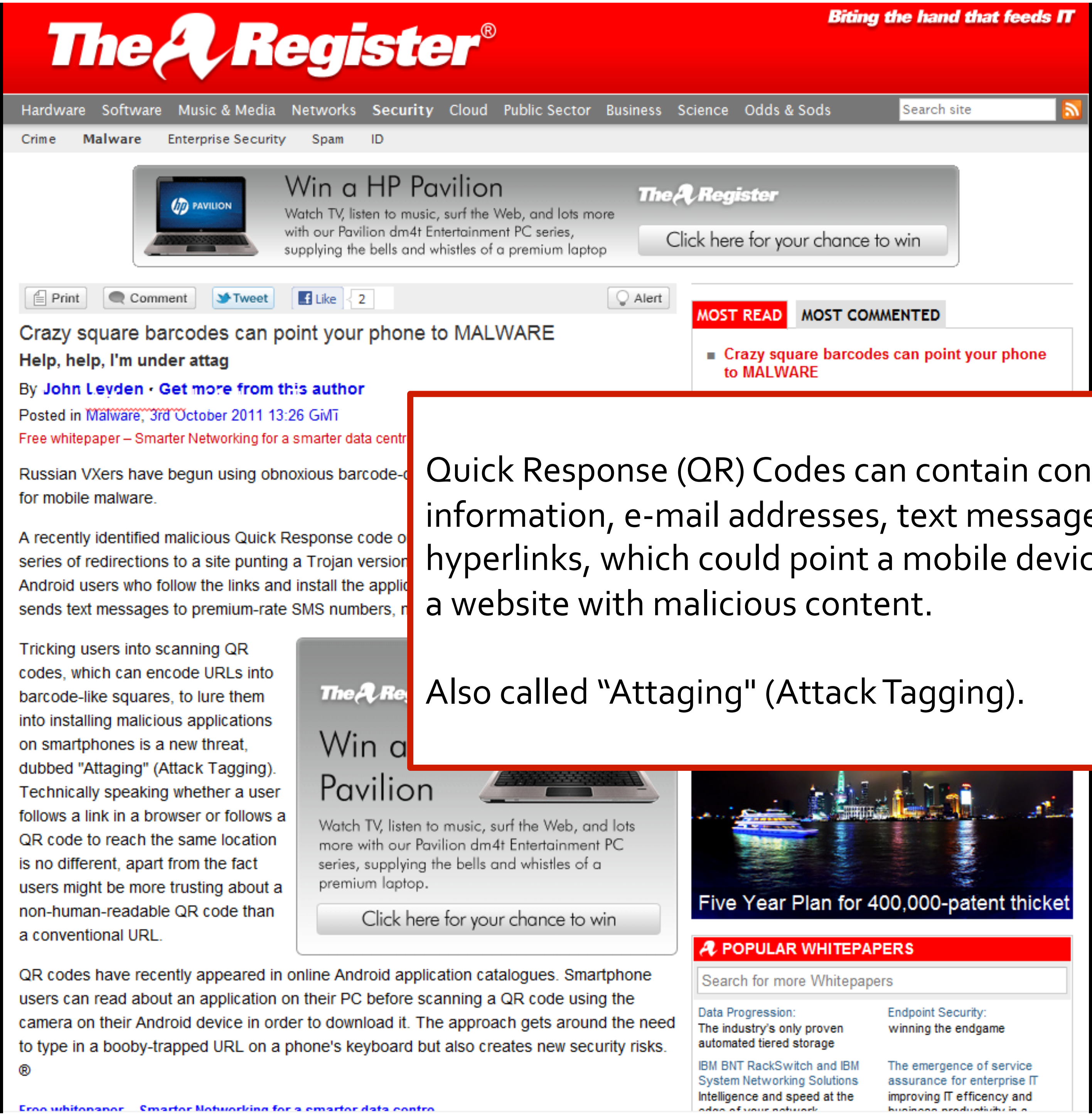
Top-Five Types of Madware Functionality
Percentage of Ad Libraries

Source: Symantec

Symantec Internet Security Threat Report 2014

Which brings me to this:

If you scan this, where will it take you?



The Register®
Biting the hand that feeds IT
Hardware Software Music & Media Networks Security Cloud Public Sector Business Science Odds & Sods
Search site
Crime Malware Enterprise Security Spam ID

Print Comment Tweet Like 2 Alert

Crazy square barcodes can point your phone to MALWARE

Help, help, I'm under attag

By **John Leyden** • **Get more from this author**

Posted in Malware, 3rd October 2011 13:26 GMT

Free whitepaper – Smarter Networking for a smarter data centr

Russian VXers have begun using obnoxious barcode-
for mobile malware.

A recently identified malicious Quick Response code o
series of redirections to a site punting a Trojan version
Android users who follow the links and install the applic
sends text messages to premium-rate SMS numbers, r

Tricking users into scanning QR codes, which can encode URLs into barcode-like squares, to lure them into installing malicious applications on smartphones is a new threat, dubbed "Attaging" (Attack Tagging). Technically speaking whether a user follows a link in a browser or follows a QR code to reach the same location is no different, apart from the fact users might be more trusting about a non-human-readable QR code than a conventional URL.

QR codes have recently appeared in online Android application catalogues. Smartphone users can read about an application on their PC before scanning a QR code using the camera on their Android device in order to download it. The approach gets around the need to type in a booby-trapped URL on a phone's keyboard but also creates new security risks. ®

Free whitepaper – Smarter Networking for a smarter data centre

- Crazy square barcodes can point your phone to MALWARE

Five Year Plan for 400,000-patent thicket

Quick Response (QR) Codes can contain contact information, e-mail addresses, text messages, or hyperlinks, which could point a mobile device to a website with malicious content.

Also called "Attaging" (Attack Tagging).

http://www.theregister.co.uk/2011/10/03/qr_code_mobile_malware_risk/

SMS Messages

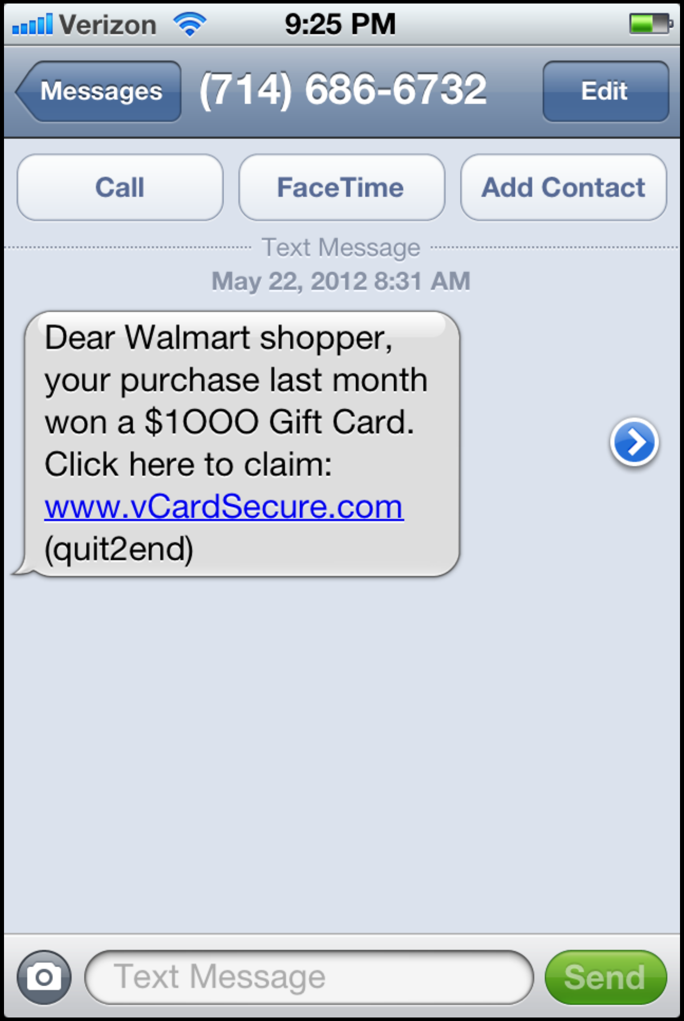
SMiShing

Consider the source?

2009 Black Hat demo: How to send spoofed SMS messages that appeared to be from the user's mobile carrier.

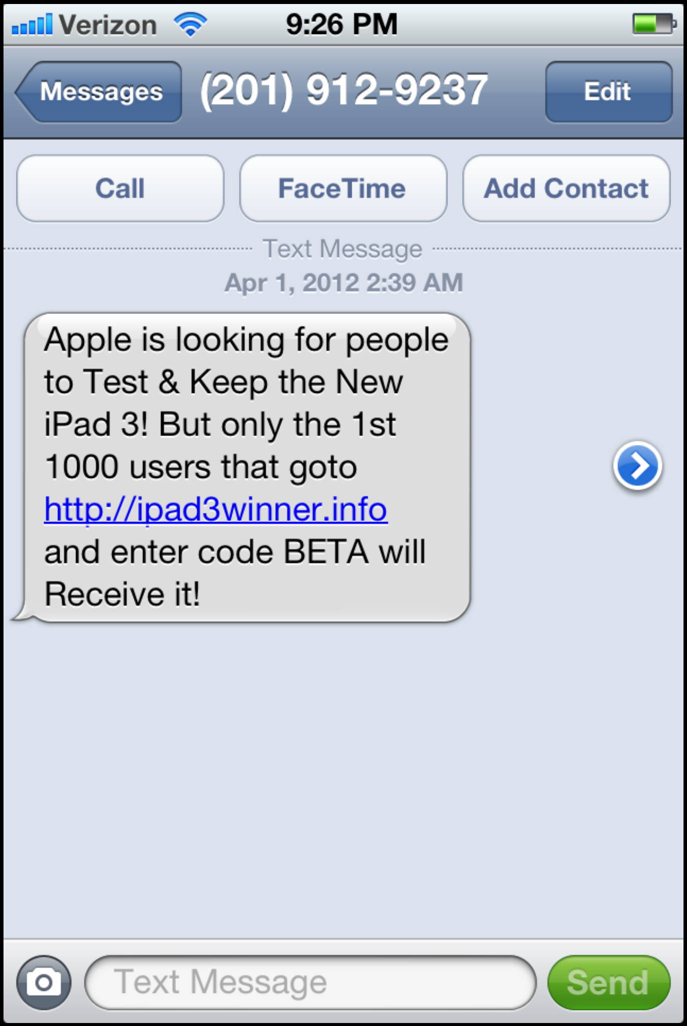
Zetter, K. (2009, July 21). "Spoofed Cell Phone Texts Post Malware Threat." http://wired.com/threatlevel/2009/07/sms/.
Image created by Stuart Miles. http://www.freedigitalphotos.net

Are these real?



May 22, 2012 8:31 AM

Dear Walmart shopper, your purchase last month won a $1OOO Gift Card. Click here to claim: www.vCardSecure.com (quit2end)

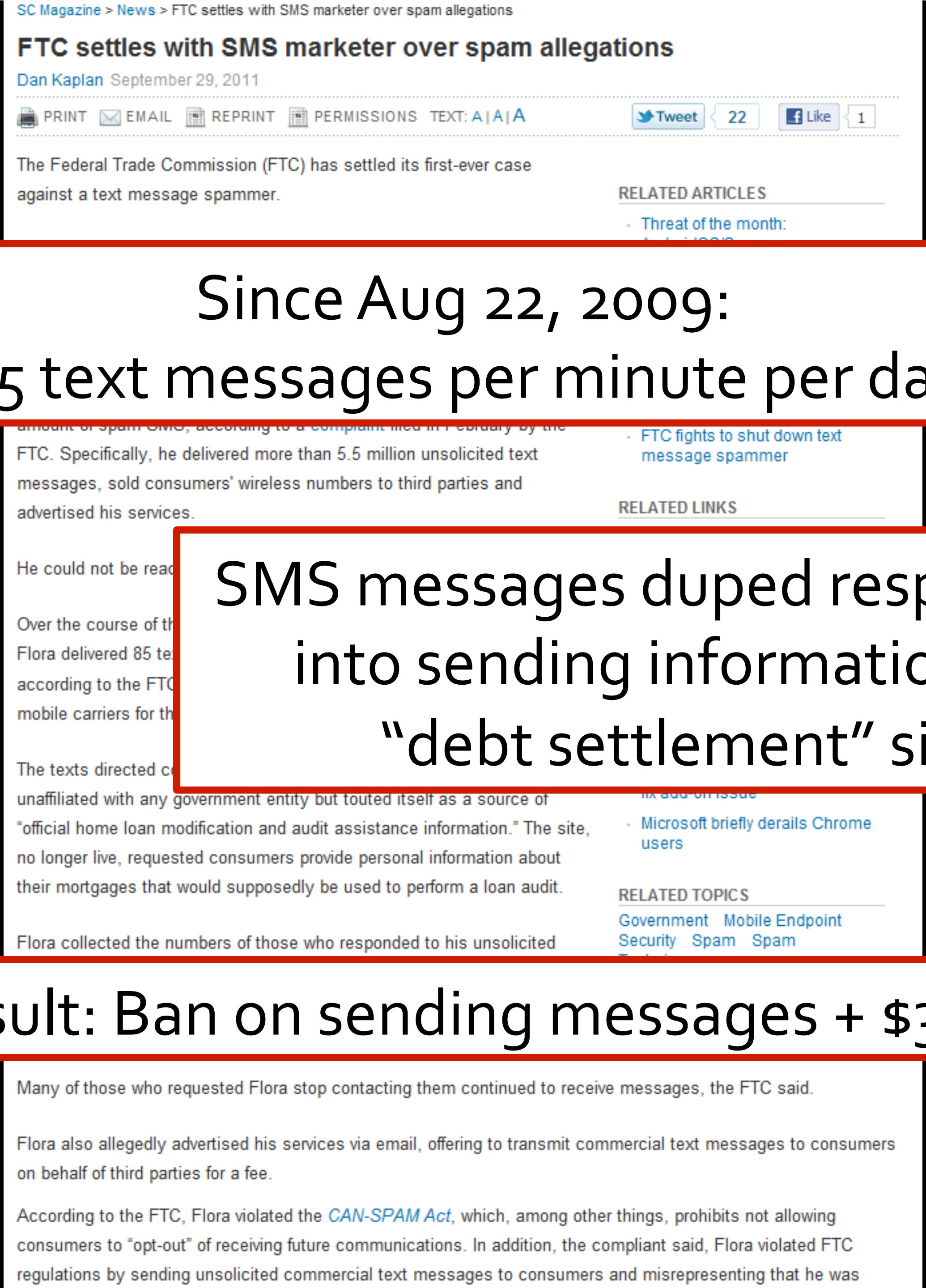


Apr 1, 2012 2:39 AM

Apple is looking for people to Test & Keep the New iPad 3! But only the 1st 1000 users that goto http://ipad3winner.info and enter code BETA will Receive it!

So how fast can you (or you kid) text?

http://www.scmagazineus.com/ftc-settles-with-sms-marketer-over-spam-allegations/article/213163/



SC Magazine > News > FTC settles with SMS marketer over spam allegations

FTC settles with SMS marketer over spam allegations

Dan Kaplan September 29, 2011

The Federal Trade Commission (FTC) has settled its first-ever case against a text message spammer.

amount of spam SMS, according to a complaint filed in February by the FTC. Specifically, he delivered more than 5.5 million unsolicited text messages, sold consumers' wireless numbers to third parties and advertised his services.

He could not be reac

Over the course of th
Flora delivered 85 te
according to the FTC
mobile carriers for th

The texts directed c
unaffiliated with any government entity but touted itself as a source of "official home loan modification and audit assistance information." The site, no longer live, requested consumers provide personal information about their mortgages that would supposedly be used to perform a loan audit.

Flora collected the numbers of those who responded to his unsolicited

Many of those who requested Flora stop contacting them continued to receive messages, the FTC said.

Flora also allegedly advertised his services via email, offering to transmit commercial text messages to consumers on behalf of third parties for a fee.

According to the FTC, Flora violated the *CAN-SPAM Act*, which, among other things, prohibits not allowing consumers to "opt-out" of receiving future communications. In addition, the compliant said, Flora violated FTC regulations by sending unsolicited commercial text messages to consumers and misrepresenting that he was

RELATED ARTICLES

- Threat of the month:
- FTC fights to shut down text message spammer

RELATED LINKS

- fix add-on issue
- Microsoft briefly derails Chrome users

RELATED TOPICS

Government Mobile Endpoint Security Spam Spam

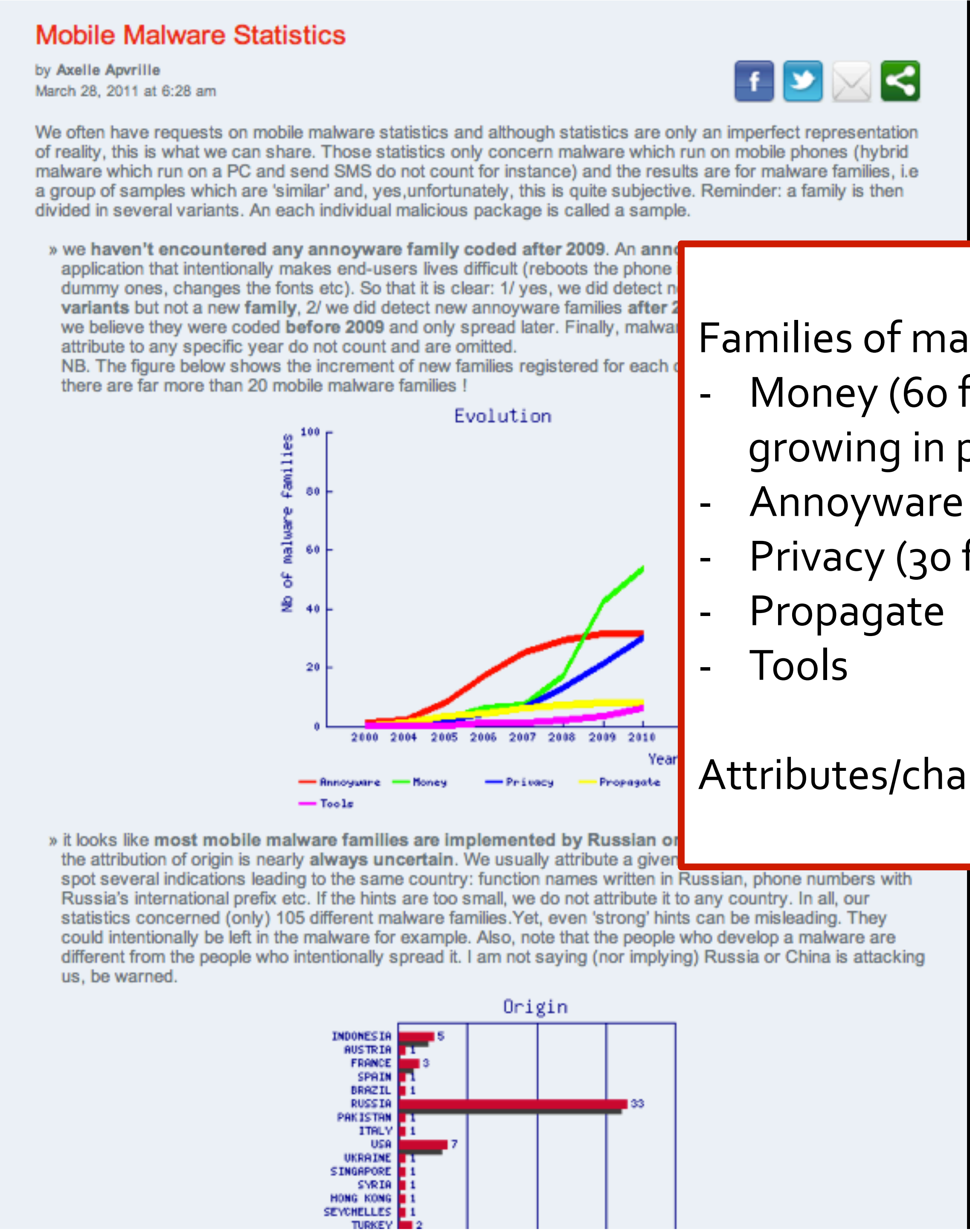
Since Aug 22, 2009:
85 text messages per minute per day

SMS messages duped respondents into sending information to a "debt settlement" site.

Result: Ban on sending messages + $32K

But really…
what kind of malware could I get from a link?

http://blog.fortinet.com/mobile-malware-statistics/



Mobile Malware Statistics

by Axelle Apvrille
March 28, 2011 at 6:28 am

We often have requests on mobile malware statistics and although statistics are only an imperfect representation of reality, this is what we can share. Those statistics only concern malware which run on mobile phones (hybrid malware which run on a PC and send SMS do not count for instance) and the results are for malware families, i.e a group of samples which are 'similar' and, yes,unfortunately, this is quite subjective. Reminder: a family is then divided in several variants. An each individual malicious package is called a sample.

» we **haven't encountered any annoyware family coded after 2009**. An anno
application that intentionally makes end-users lives difficult (reboots the phone
dummy ones, changes the fonts etc). So that it is clear: 1/ yes, we did detect n
variants but not a new **family**, 2/ we did detect new annoyware families **after 2**
we believe they were coded **before 2009** and only spread later. Finally, malwar
attribute to any specific year do not count and are omitted.
NB. The figure below shows the increment of new families registered for each
there are far more than 20 mobile malware families !

» it looks like **most mobile malware families are implemented by Russian or**
the attribution of origin is nearly **always uncertain**. We usually attribute a given
spot several indications leading to the same country: function names written in Russian, phone numbers with Russia's international prefix etc. If the hints are too small, we do not attribute it to any country. In all, our statistics concerned (only) 105 different malware families.Yet, even 'strong' hints can be misleading. They could intentionally be left in the malware for example. Also, note that the people who develop a malware are different from the people who intentionally spread it. I am not saying (nor implying) Russia or China is attacking us, be warned.

Families of malware:

- Money (60 families – growing in popularity)
- Annoyware (30 families)
- Privacy (30 families)
- Propagate
- Tools

Attributes/characteristics

Infection Methods by Platform

J2ME

- Chat/IM
- Games
- Adult Entertainment

Symbian

- Chat/IM

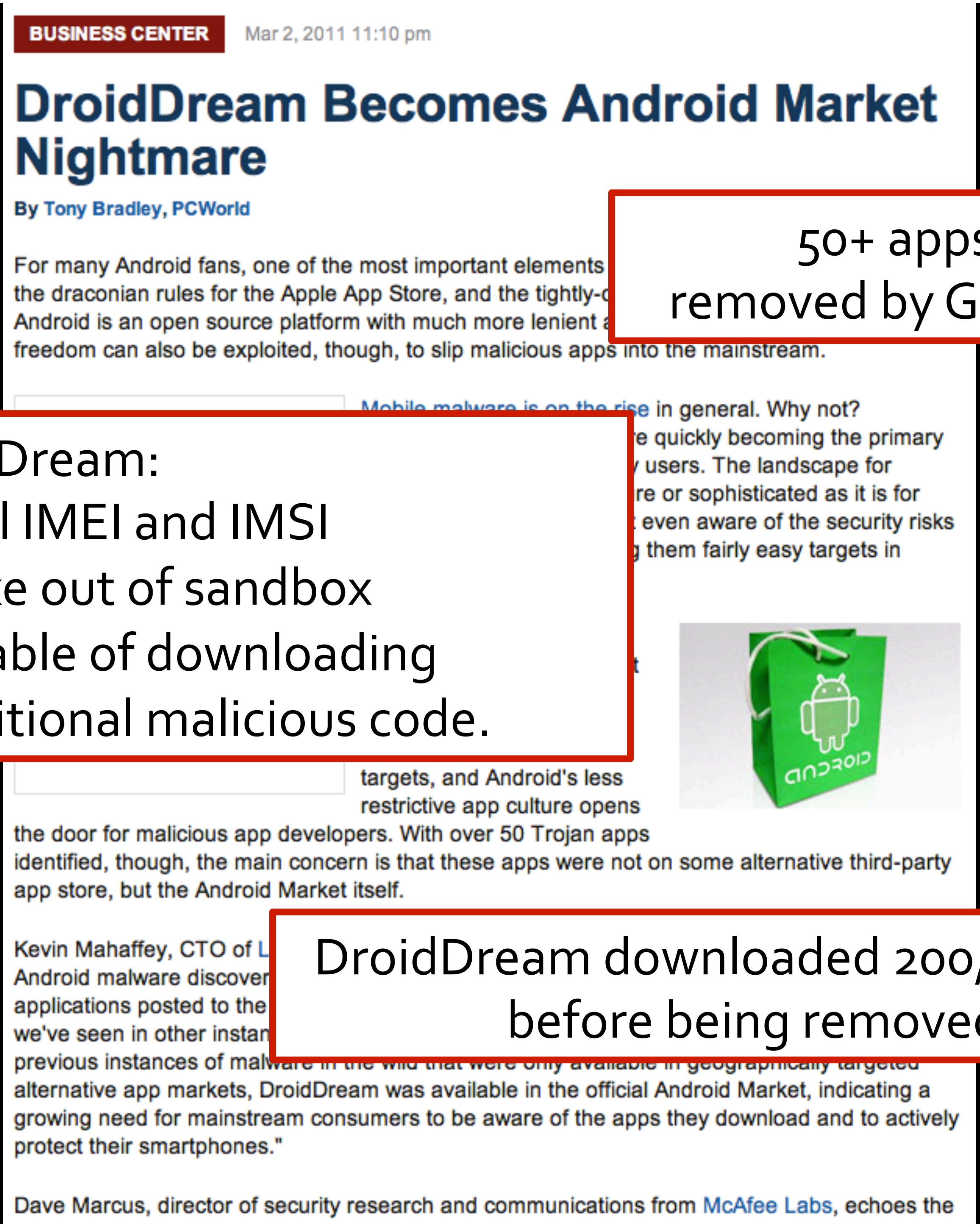
Android

- Apps/Games
- Chat/IM
- Web 2.0 sites, e.g., social networking sites
- Changing approaches

Targets

- Send SMS texts to premium services

- Steal information
  - SIM Card
  - Personal
  - Financial
  - Corporate data



BUSINESS CENTER Mar 2, 2011 11:10 pm

DroidDream Becomes Android Market Nightmare

By Tony Bradley, PCWorld

For many Android fans, one of the most important elements
the draconian rules for the Apple App Store, and the tightly-c
Android is an open source platform with much more lenient a
freedom can also be exploited, though, to slip malicious apps into the mainstream.

Mobile malware is on the rise in general. Why not?
e quickly becoming the primary
y users. The landscape for
re or sophisticated as it is for
t even aware of the security risks
g them fairly easy targets in

t

targets, and Android's less restrictive app culture opens the door for malicious app developers. With over 50 Trojan apps identified, though, the main concern is that these apps were not on some alternative third-party app store, but the Android Market itself.

Kevin Mahaffey, CTO of L
Android malware discover
applications posted to the
we've seen in other instan
previous instances of malware in the wild that were only available in geographically targeted alternative app markets, DroidDream was available in the official Android Market, indicating a growing need for mainstream consumers to be aware of the apps they download and to actively protect their smartphones."

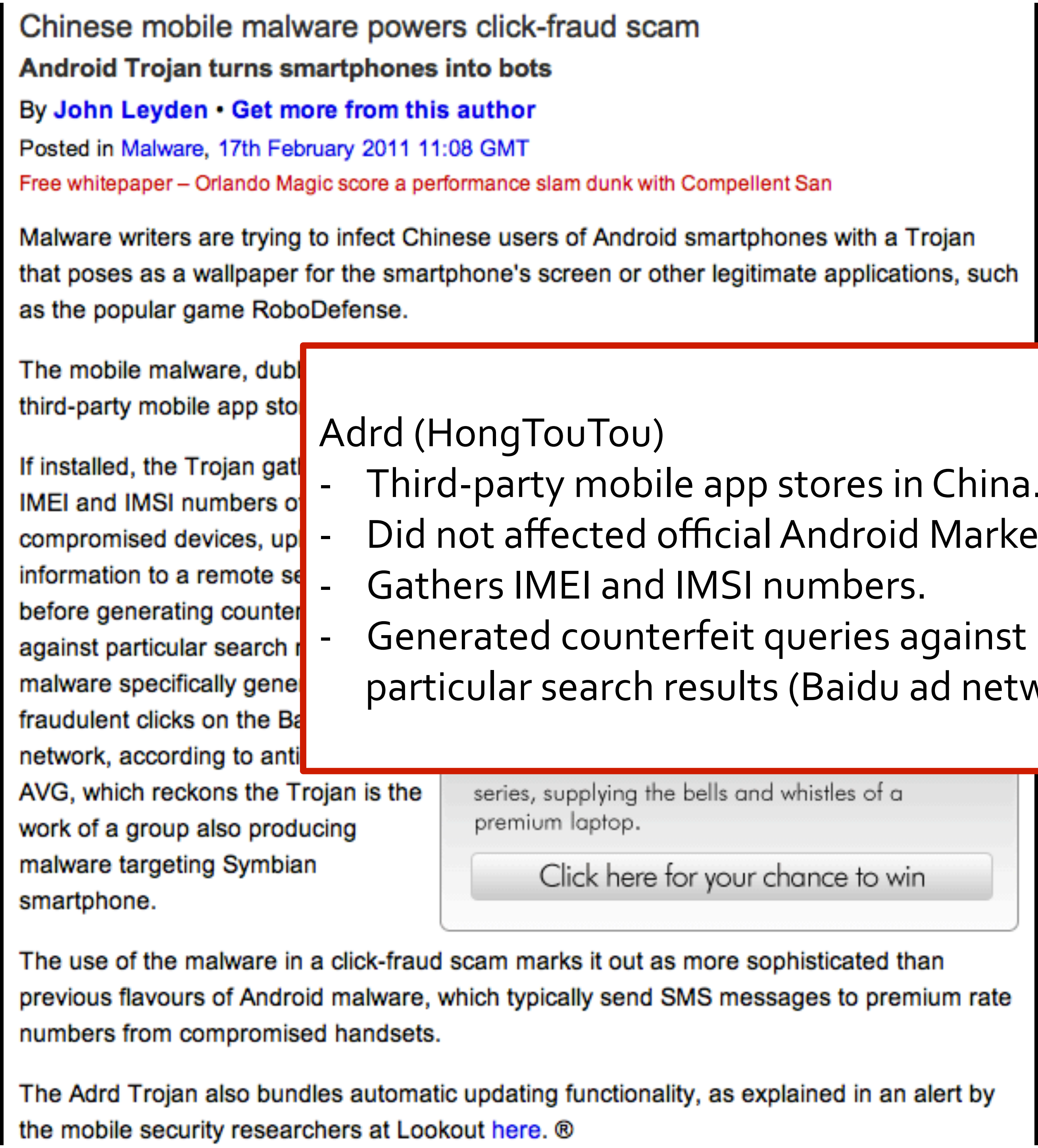
Dave Marcus, director of security research and communications from McAfee Labs, echoes the

50+ apps
removed by Google.

DroidDream:
- Steal IMEI and IMSI
- Broke out of sandbox
- Capable of downloading
  additional malicious code.

DroidDream downloaded 200,000 times
before being removed.

http://www.pcworld.com/businesscenter/article/221247/droiddream_becomes_android_market_nightmare.html



Chinese mobile malware powers click-fraud scam

Android Trojan turns smartphones into bots

By John Leyden • Get more from this author

Posted in Malware, 17th February 2011 11:08 GMT

Malware writers are trying to infect Chinese users of Android smartphones with a Trojan that poses as a wallpaper for the smartphone's screen or other legitimate applications, such as the popular game RoboDefense.

The mobile malware, dubl
third-party mobile app sto

If installed, the Trojan gatl
IMEI and IMSI numbers o
compromised devices, up
information to a remote se
before generating counter
against particular search r
malware specifically gene
fraudulent clicks on the Ba
network, according to anti
AVG, which reckons the Trojan is the
work of a group also producing
malware targeting Symbian
smartphone.

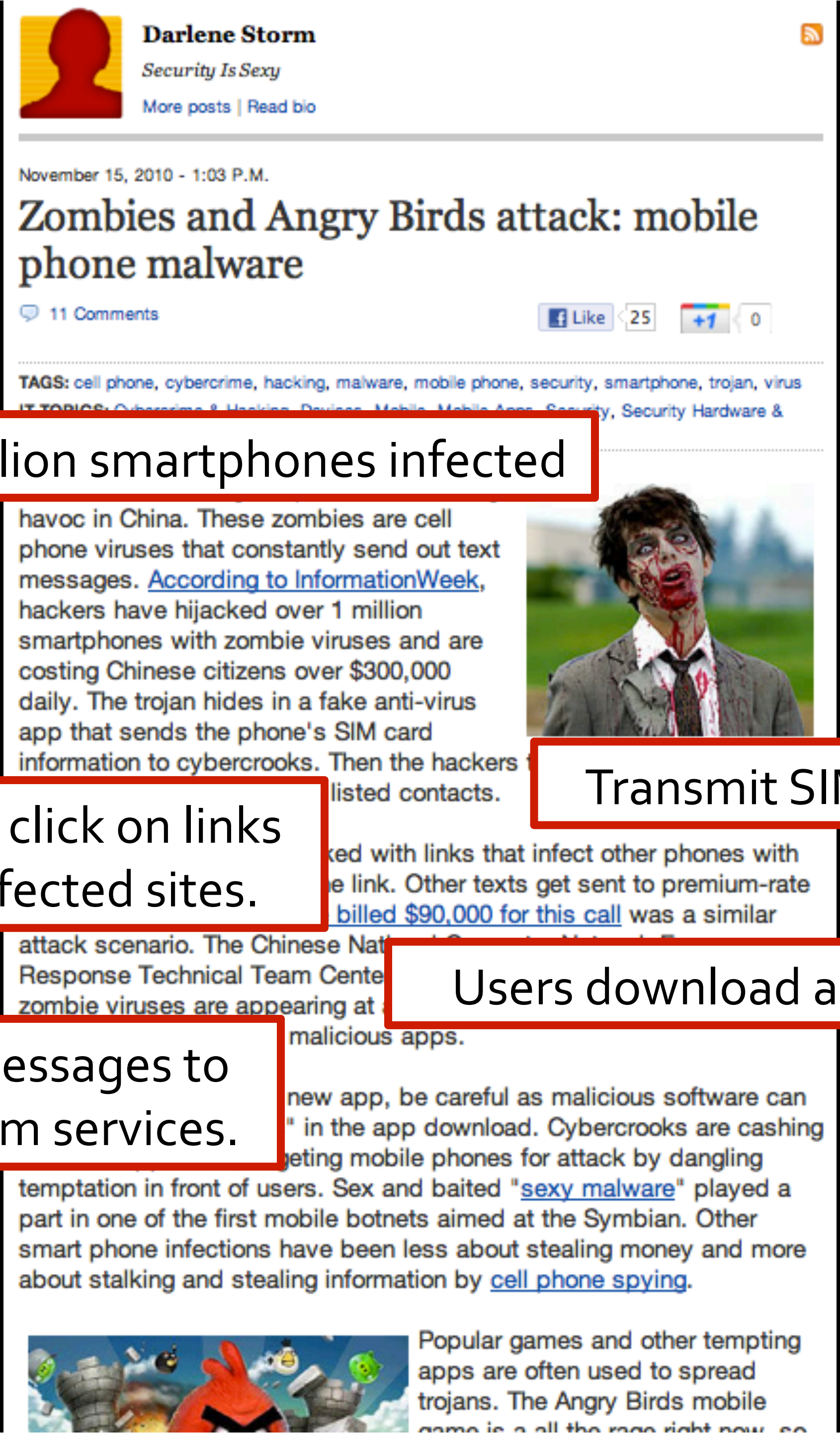
The use of the malware in a click-fraud scam marks it out as more sophisticated than previous flavours of Android malware, which typically send SMS messages to premium rate numbers from compromised handsets.

The Adrd Trojan also bundles automatic updating functionality, as explained in an alert by the mobile security researchers at Lookout here. ®

Adrd (HongTouTou)

- Third-party mobile app stores in China.
- Did not affected official Android Market.
- Gathers IMEI and IMSI numbers.
- Generated counterfeit queries against particular search results (Baidu ad network).

http://www.theregister.co.uk/2011/02/17/android_trojan_click_fraud_scam/



Darlene Storm

Security Is Sexy

More posts | Read bio

November 15, 2010 - 1:03 P.M.

Zombies and Angry Birds attack: mobile phone malware

11 Comments

Like 25 +1 0

TAGS: cell phone, cybercrime, hacking, malware, mobile phone, security, smartphone, trojan, virus

IT TOPICS: Cybercrime & Hacking, Devices, Mobile, Mobile Apps, Security, Security Hardware &

havoc in China. These zombies are cell phone viruses that constantly send out text messages. According to InformationWeek, hackers have hijacked over 1 million smartphones with zombie viruses and are costing Chinese citizens over $300,000 daily. The trojan hides in a fake anti-virus app that sends the phone's SIM card information to cybercrooks. Then the hackers t listed contacts.

ked with links that infect other phones with e link. Other texts get sent to premium-rate billed $90,000 for this call was a similar attack scenario. The Chinese Nat Response Technical Team Cente zombie viruses are appearing at malicious apps.

new app, be careful as malicious software can " in the app download. Cybercrooks are cashing geting mobile phones for attack by dangling temptation in front of users. Sex and baited "sexy malware" played a part in one of the first mobile botnets aimed at the Symbian. Other smart phone infections have been less about stealing money and more about stalking and stealing information by cell phone spying.

Popular games and other tempting apps are often used to spread trojans. The Angry Birds mobile game is a all the rage right now, so

Over 1 million smartphones infected

Transmit SIM card data

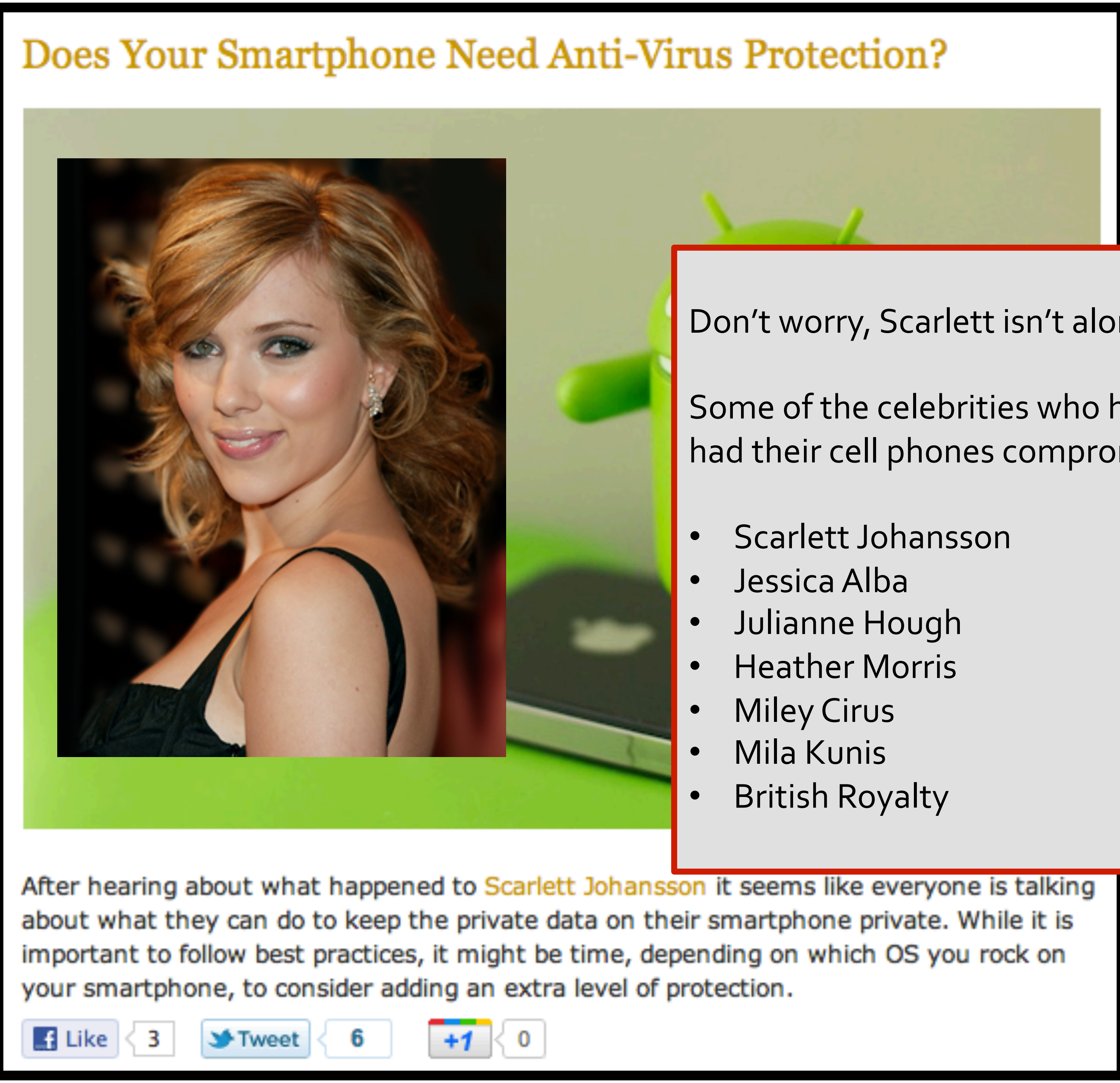
Users click on links to infected sites.

Users download apps.

Text messages to premium services.

http://blogs.computerworld.com/17355/zombies_and_angry_birds_attack_mobile_phone_malware

Moving beyond names and passwords.



Does Your Smartphone Need Anti-Virus Protection?

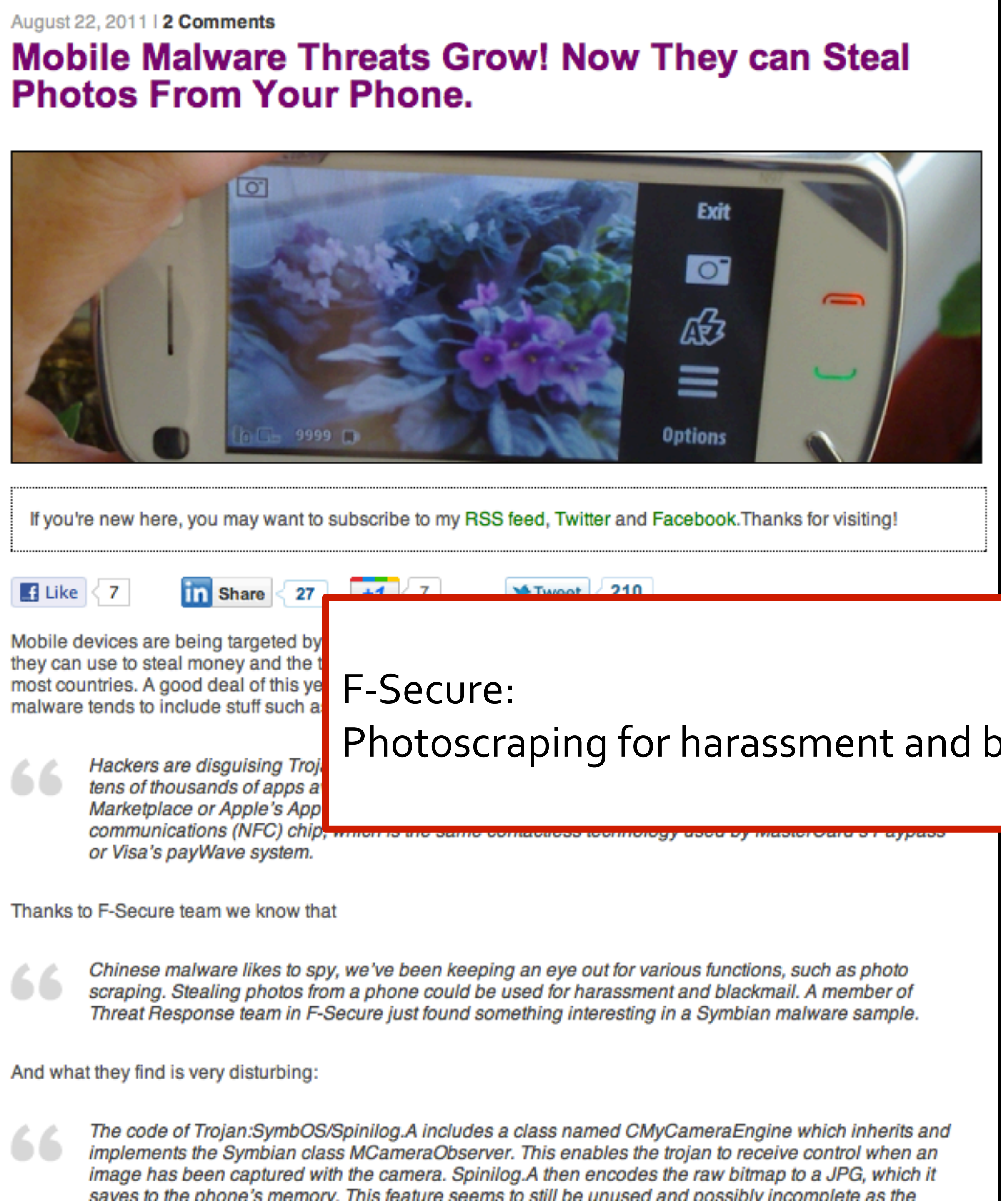
After hearing about what happened to Scarlett Johansson it seems like everyone is talking about what they can do to keep the private data on their smartphone private. While it is important to follow best practices, it might be time, depending on which OS you rock on your smartphone, to consider adding an extra level of protection.

Don't worry, Scarlett isn't alone.

Some of the celebrities who have had their cell phones compromised.

- Scarlett Johansson
- Jessica Alba
- Julianne Hough
- Heather Morris
- Miley Cirus
- Mila Kunis
- British Royalty

http://www.unplggd.com/unplggd/safety-security/does-your-smartphone-need-antivirus-protection-156222 http://slashnext.com/2011/08/mobile-malware-threats-grow-now-they-can-steal-photos-from-your-phone/



August 22, 2011 | **2 Comments**

Mobile Malware Threats Grow! Now They can Steal Photos From Your Phone.

If you're new here, you may want to subscribe to my RSS feed, Twitter and Facebook.Thanks for visiting!

Mobile devices are being targeted by
they can use to steal money and the t
most countries. A good deal of this ye
malware tends to include stuff such a

> *Hackers are disguising Troj*
> *tens of thousands of apps a*
> *Marketplace or Apple's App*
> *communications (NFC) chip, which is the same contactless technology used by MasterCard's Paypass or Visa's payWave system.*

Thanks to F-Secure team we know that

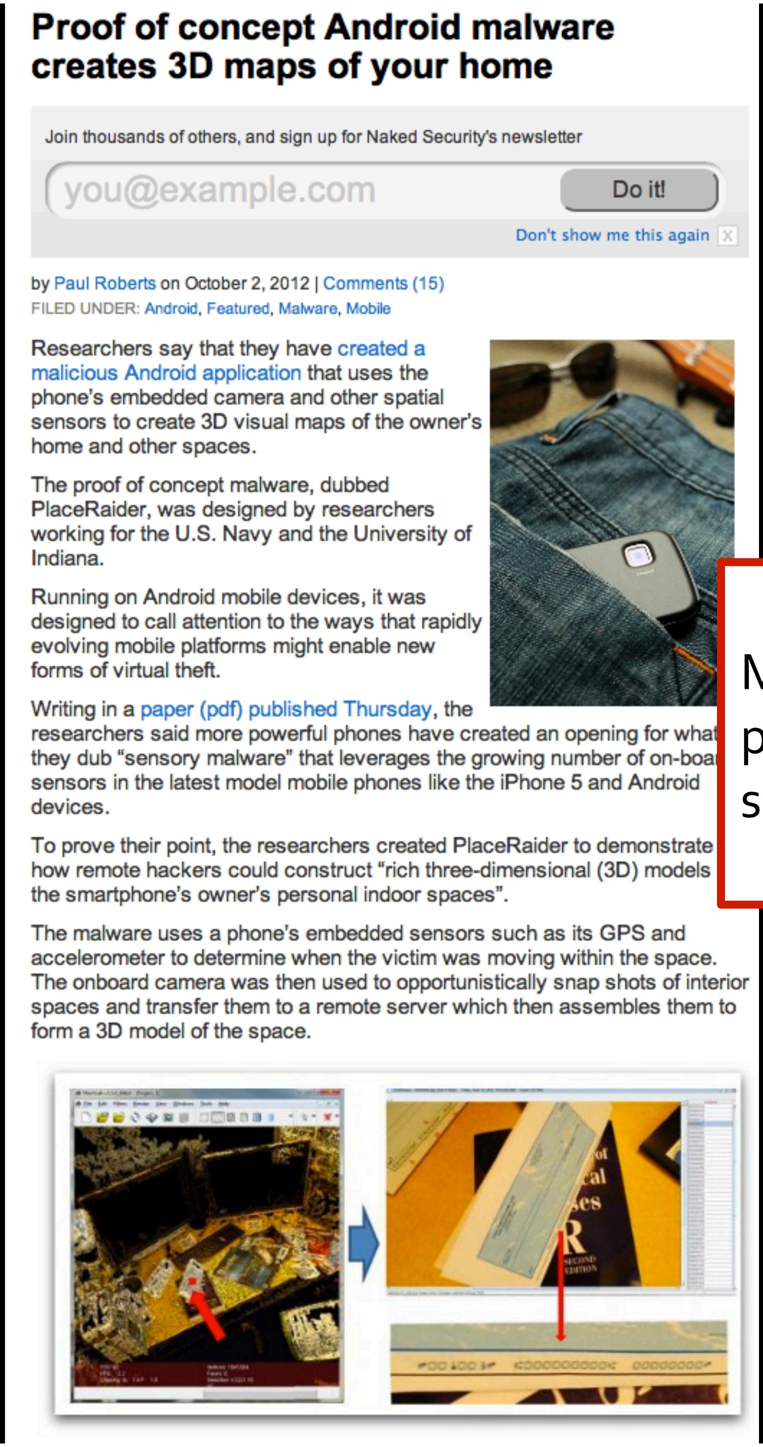
> *Chinese malware likes to spy, we've been keeping an eye out for various functions, such as photo scraping. Stealing photos from a phone could be used for harassment and blackmail. A member of Threat Response team in F-Secure just found something interesting in a Symbian malware sample.*

And what they find is very disturbing:

> *The code of Trojan:SymbOS/Spinilog.A includes a class named CMyCameraEngine which inherits and implements the Symbian class MCameraObserver. This enables the trojan to receive control when an image has been captured with the camera. Spinilog.A then encodes the raw bitmap to a JPG, which it saves to the phone's memory. This feature seems to still be unused and possibly incomplete as the*

F-Secure:
Photoscraping for harassment and blackmail.

http://nakedsecurity.sophos.com/2012/10/02/proof-of-concept-android-malware-creates-3d-maps-of-your-home/



Proof of concept Android malware creates 3D maps of your home

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com Do it!

Don't show me this again

by Paul Roberts on October 2, 2012 | Comments (15)
FILED UNDER: Android, Featured, Malware, Mobile

Researchers say that they have created a malicious Android application that uses the phone's embedded camera and other spatial sensors to create 3D visual maps of the owner's home and other spaces.

The proof of concept malware, dubbed PlaceRaider, was designed by researchers working for the U.S. Navy and the University of Indiana.

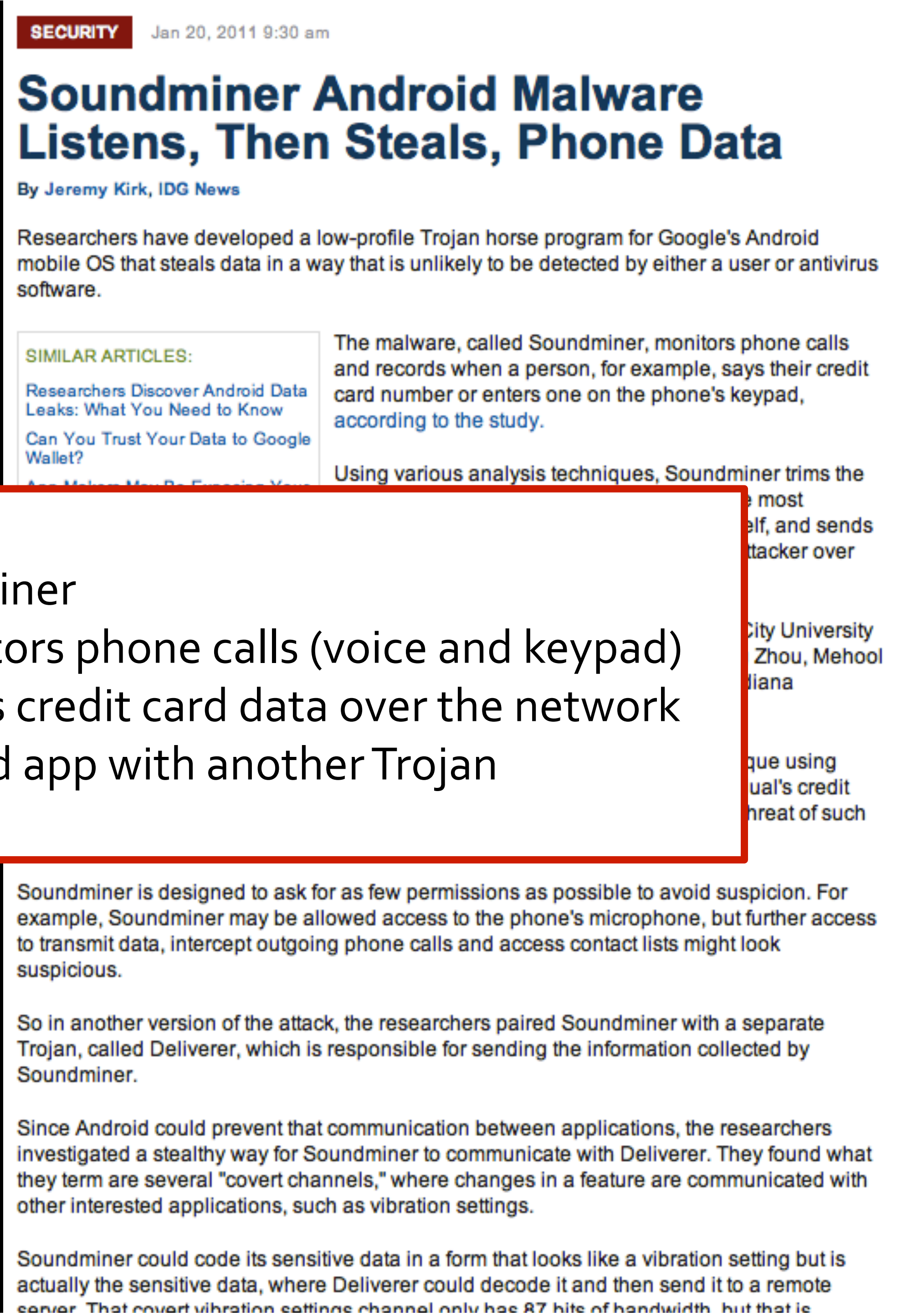
Running on Android mobile devices, it was designed to call attention to the ways that rapidly evolving mobile platforms might enable new forms of virtual theft.

Writing in a paper (pdf) published Thursday, the researchers said more powerful phones have created an opening for what they dub "sensory malware" that leverages the growing number of on-boar sensors in the latest model mobile phones like the iPhone 5 and Android devices.

To prove their point, the researchers created PlaceRaider to demonstrate how remote hackers could construct "rich three-dimensional (3D) models the smartphone's owner's personal indoor spaces".

The malware uses a phone's embedded sensors such as its GPS and accelerometer to determine when the victim was moving within the space. The onboard camera was then used to opportunistically snap shots of interior spaces and transfer them to a remote server which then assembles them to form a 3D model of the space.

Malware can "stitch together" pictures to form a map of the surroundings.



SECURITY Jan 20, 2011 9:30 am

Soundminer Android Malware Listens, Then Steals, Phone Data

By Jeremy Kirk, IDG News

Researchers have developed a low-profile Trojan horse program for Google's Android mobile OS that steals data in a way that is unlikely to be detected by either a user or antivirus software.

SIMILAR ARTICLES:

Researchers Discover Android Data Leaks: What You Need to Know

Can You Trust Your Data to Google Wallet?

App Makers May Be Exposing Your

The malware, called Soundminer, monitors phone calls and records when a person, for example, says their credit card number or enters one on the phone's keypad, according to the study.

Using various analysis techniques, Soundminer trims the

e most

elf, and sends

ttacker over

City University

Zhou, Mehool

diana

que using

ual's credit

hreat of such

Soundminer is designed to ask for as few permissions as possible to avoid suspicion. For example, Soundminer may be allowed access to the phone's microphone, but further access to transmit data, intercept outgoing phone calls and access contact lists might look suspicious.

So in another version of the attack, the researchers paired Soundminer with a separate Trojan, called Deliverer, which is responsible for sending the information collected by Soundminer.

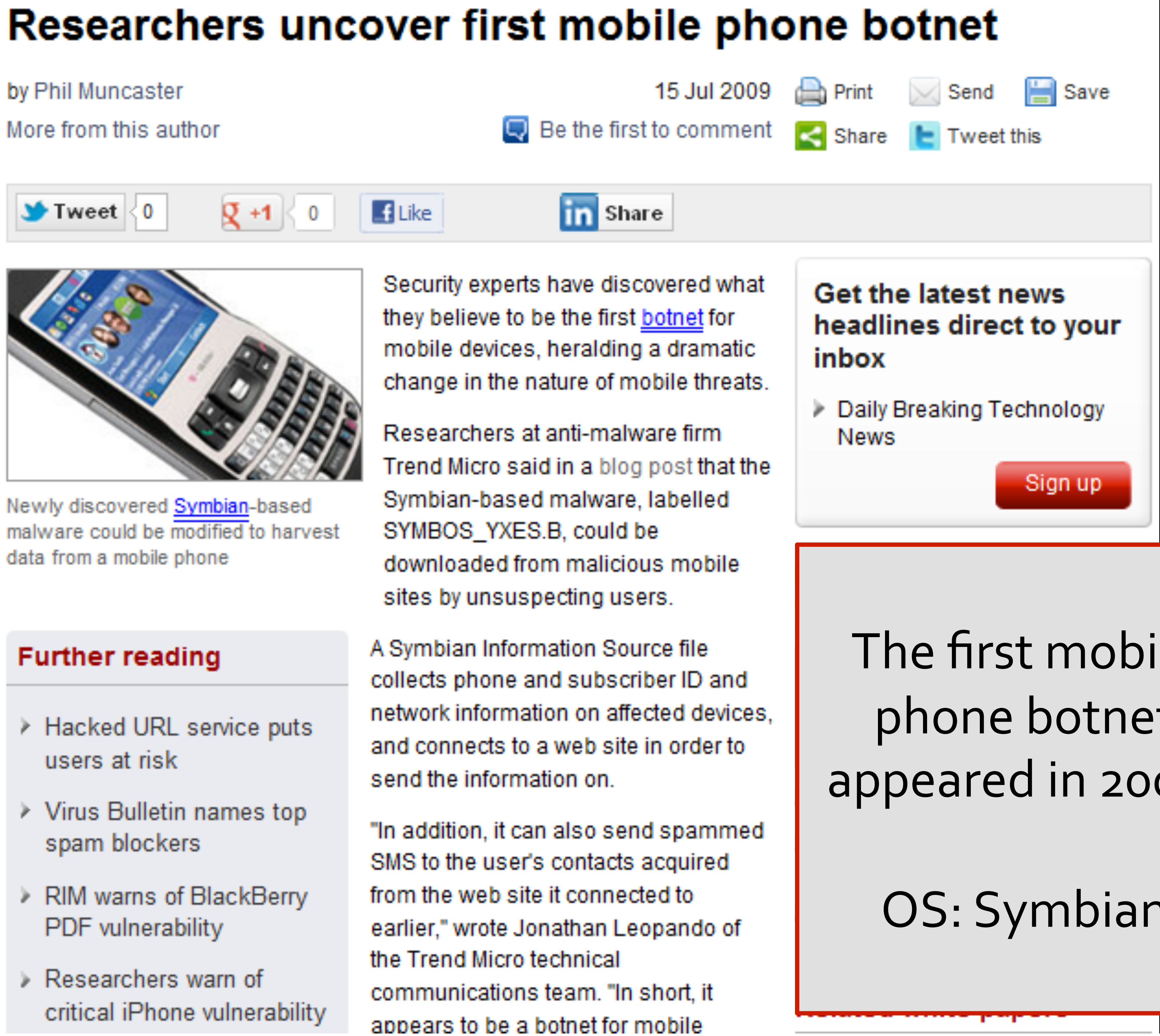
Since Android could prevent that communication between applications, the researchers investigated a stealthy way for Soundminer to communicate with Deliverer. They found what they term are several "covert channels," where changes in a feature are communicated with other interested applications, such as vibration settings.

Soundminer could code its sensitive data in a form that looks like a vibration setting but is actually the sensitive data, where Deliverer could decode it and then send it to a remote server. That covert vibration settings channel only has 87 bits of bandwidth, but that is

Soundminer
- Monitors phone calls (voice and keypad)
- Sends credit card data over the network
- Paired app with another Trojan

http://www.pcworld.com/businesscenter/article/217133/
soundminer_android_malware_listens_then_steals_phone_data.html

And then there are botnets.



Researchers uncover first mobile phone botnet

by Phil Muncaster

More from this author

15 Jul 2009

Be the first to comment

Newly discovered Symbian-based malware could be modified to harvest data from a mobile phone

Security experts have discovered what they believe to be the first botnet for mobile devices, heralding a dramatic change in the nature of mobile threats.

Researchers at anti-malware firm Trend Micro said in a blog post that the Symbian-based malware, labelled SYMBOS_YXES.B, could be downloaded from malicious mobile sites by unsuspecting users.

A Symbian Information Source file collects phone and subscriber ID and network information on affected devices, and connects to a web site in order to send the information on.

"In addition, it can also send spammed SMS to the user's contacts acquired from the web site it connected to earlier," wrote Jonathan Leopando of the Trend Micro technical communications team. "In short, it appears to be a botnet for mobile

Get the latest news headlines direct to your inbox

- Daily Breaking Technology News

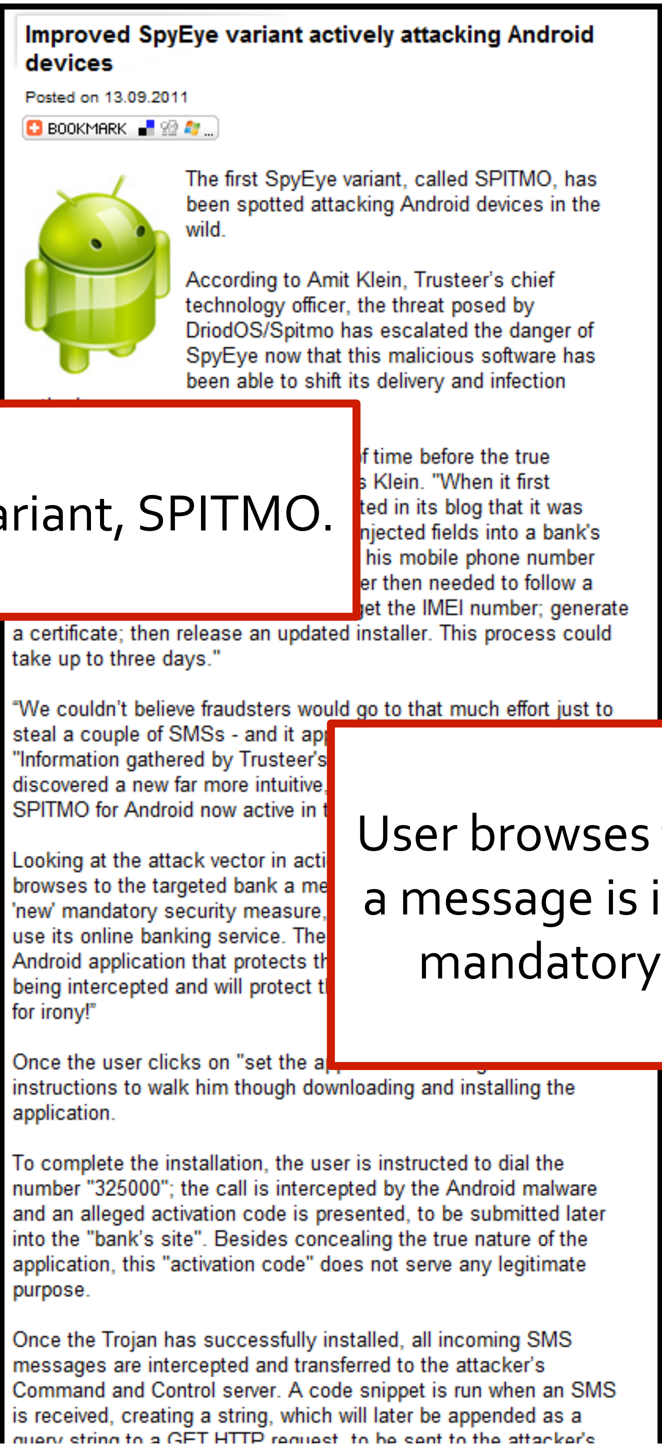
Further reading

- Hacked URL service puts users at risk
- Virus Bulletin names top spam blockers
- RIM warns of BlackBerry PDF vulnerability
- Researchers warn of critical iPhone vulnerability

The first mobile phone botnet appeared in 2009.

OS: Symbian

http://www.v3.co.uk/v3-uk/news/1993430/researchers-uncover-mobile-phone-botnet http://www.net-security.org/malware_news.php?id=1835



Improved SpyEye variant actively attacking Android devices

Posted on 13.09.2011

The first SpyEye variant, called SPITMO, has been spotted attacking Android devices in the wild.

According to Amit Klein, Trusteer's chief technology officer, the threat posed by DriodOS/Spitmo has escalated the danger of SpyEye now that this malicious software has been able to shift its delivery and infection

f time before the true
s Klein. "When it first
ted in its blog that it was
njected fields into a bank's
his mobile phone number
er then needed to follow a
jet the IMEI number; generate
a certificate; then release an updated installer. This process could take up to three days."

"We couldn't believe fraudsters would go to that much effort just to
steal a couple of SMSs - and it ap
"Information gathered by Trusteer's
discovered a new far more intuitive,
SPITMO for Android now active in t

Looking at the attack vector in acti
browses to the targeted bank a me
'new' mandatory security measure,
use its online banking service. The
Android application that protects th
being intercepted and will protect t
for irony!"

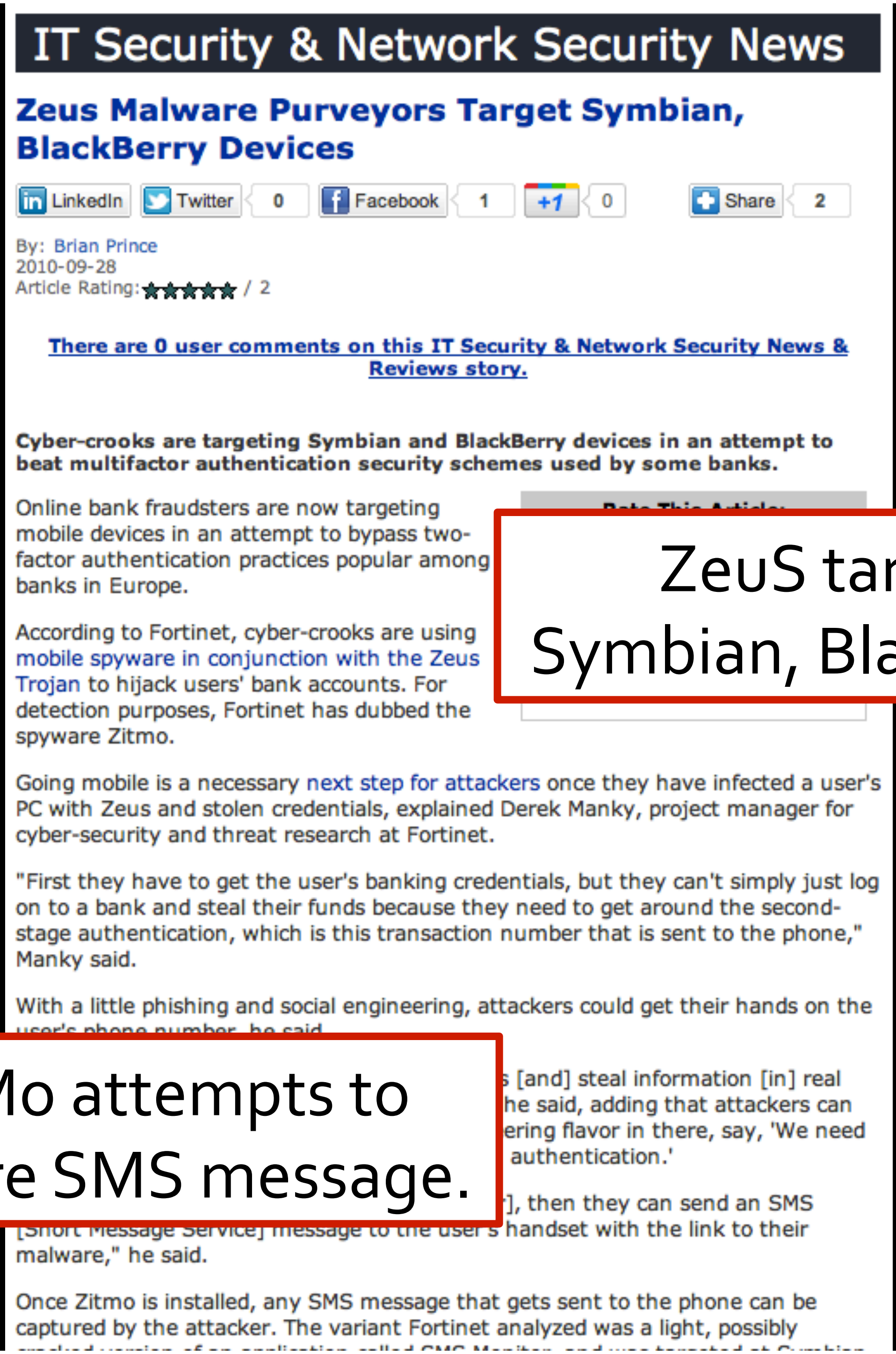
Once the user clicks on "set the a
instructions to walk him though downloading and installing the application.

To complete the installation, the user is instructed to dial the number "325000"; the call is intercepted by the Android malware and an alleged activation code is presented, to be submitted later into the "bank's site". Besides concealing the true nature of the application, this "activation code" does not serve any legitimate purpose.

Once the Trojan has successfully installed, all incoming SMS messages are intercepted and transferred to the attacker's Command and Control server. A code snippet is run when an SMS is received, creating a string, which will later be appended as a query string to a GET HTTP request, to be sent to the attacker's

Improved SpyEye variant, SPITMO.

User browses to targeted bank and a message is injected with a “new” mandatory security measure.



IT Security & Network Security News

Zeus Malware Purveyors Target Symbian, BlackBerry Devices

By: Brian Prince
2010-09-28
Article Rating: ★★★★★ / 2

There are 0 user comments on this IT Security & Network Security News & Reviews story.

Cyber-crooks are targeting Symbian and BlackBerry devices in an attempt to beat multifactor authentication security schemes used by some banks.

Rate This Article:

Online bank fraudsters are now targeting mobile devices in an attempt to bypass two-factor authentication practices popular among banks in Europe.

According to Fortinet, cyber-crooks are using mobile spyware in conjunction with the Zeus Trojan to hijack users' bank accounts. For detection purposes, Fortinet has dubbed the spyware Zitmo.

Going mobile is a necessary next step for attackers once they have infected a user's PC with Zeus and stolen credentials, explained Derek Manky, project manager for cyber-security and threat research at Fortinet.

"First they have to get the user's banking credentials, but they can't simply just log on to a bank and steal their funds because they need to get around the second-stage authentication, which is this transaction number that is sent to the phone," Manky said.

With a little phishing and social engineering, attackers could get their hands on the user's phone number, he said.

s [and] steal information [in] real
he said, adding that attackers can
ering flavor in there, say, 'We need
authentication.'

], then they can send an SMS [Short Message Service] message to the user's handset with the link to their malware," he said.

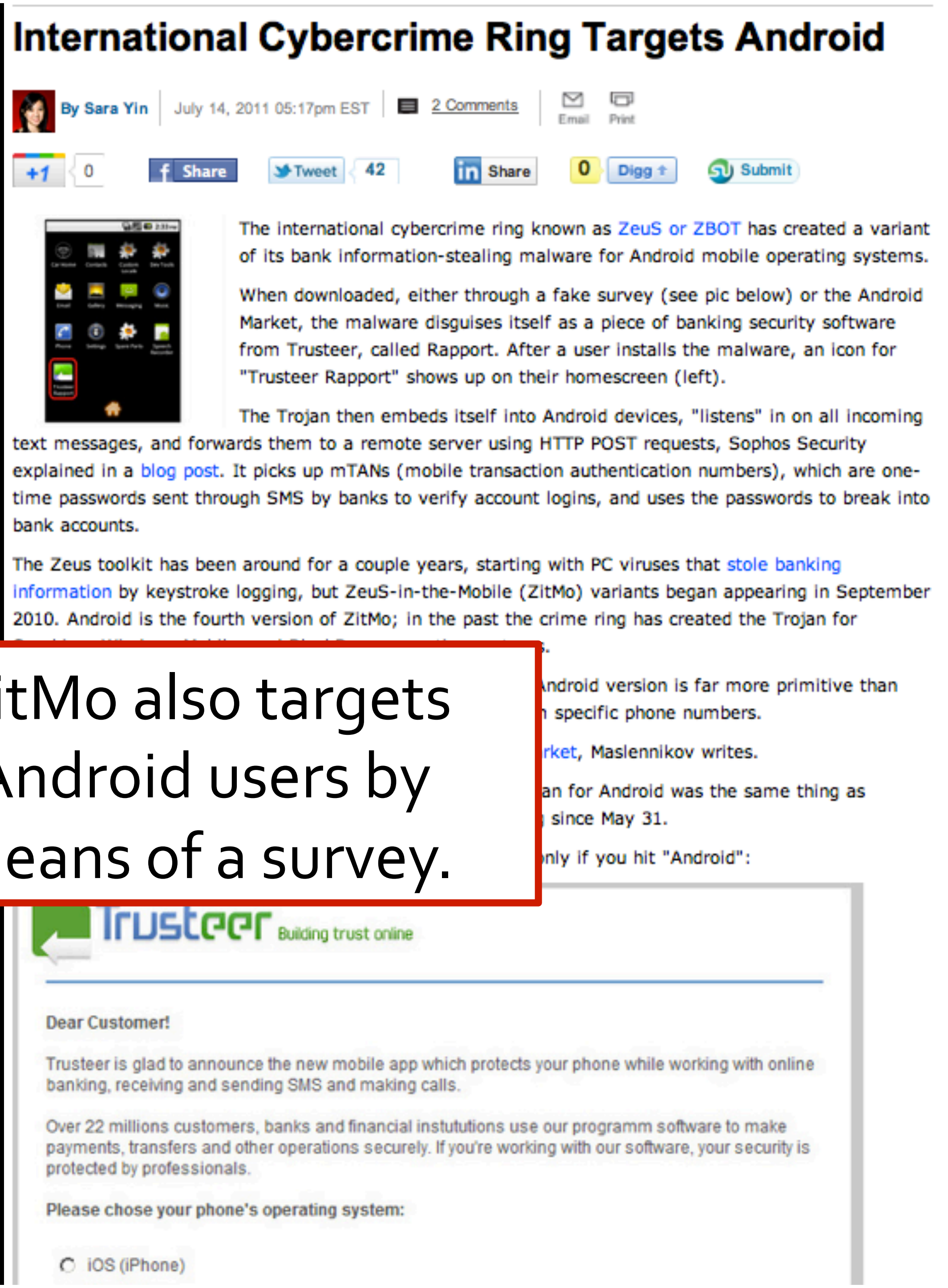
Once Zitmo is installed, any SMS message that gets sent to the phone can be captured by the attacker. The variant Fortinet analyzed was a light, possibly

ZeuS targets:
Symbian, BlackBerries

ZitMo attempts to
capture SMS message.

http://www.eweek.com/c/a/Security/Zeus-Malware-Purveyors-Target-Symbian-BlackBerry-Devices-800557/

http://www.pcmag.com/article2/0,2817,2388531,00.asp#fbid=yaVbLzb761J



International Cybercrime Ring Targets Android

By Sara Yin | July 14, 2011 05:17pm EST | 2 Comments

The international cybercrime ring known as ZeuS or ZBOT has created a variant of its bank information-stealing malware for Android mobile operating systems.

When downloaded, either through a fake survey (see pic below) or the Android Market, the malware disguises itself as a piece of banking security software from Trusteer, called Rapport. After a user installs the malware, an icon for "Trusteer Rapport" shows up on their homescreen (left).

The Trojan then embeds itself into Android devices, "listens" in on all incoming text messages, and forwards them to a remote server using HTTP POST requests, Sophos Security explained in a blog post. It picks up mTANs (mobile transaction authentication numbers), which are one-time passwords sent through SMS by banks to verify account logins, and uses the passwords to break into bank accounts.

The Zeus toolkit has been around for a couple years, starting with PC viruses that stole banking information by keystroke logging, but ZeuS-in-the-Mobile (ZitMo) variants began appearing in September 2010. Android is the fourth version of ZitMo; in the past the crime ring has created the Trojan for

s.

ndroid version is far more primitive than

n specific phone numbers.

rket, Maslennikov writes.

an for Android was the same thing as

since May 31.

nly if you hit "Android":

Trusteer Building trust online

Dear Customer!

Trusteer is glad to announce the new mobile app which protects your phone while working with online banking, receiving and sending SMS and making calls.

Over 22 millions customers, banks and financial instututions use our programm software to make payments, transfers and other operations securely. If you're working with our software, your security is protected by professionals.

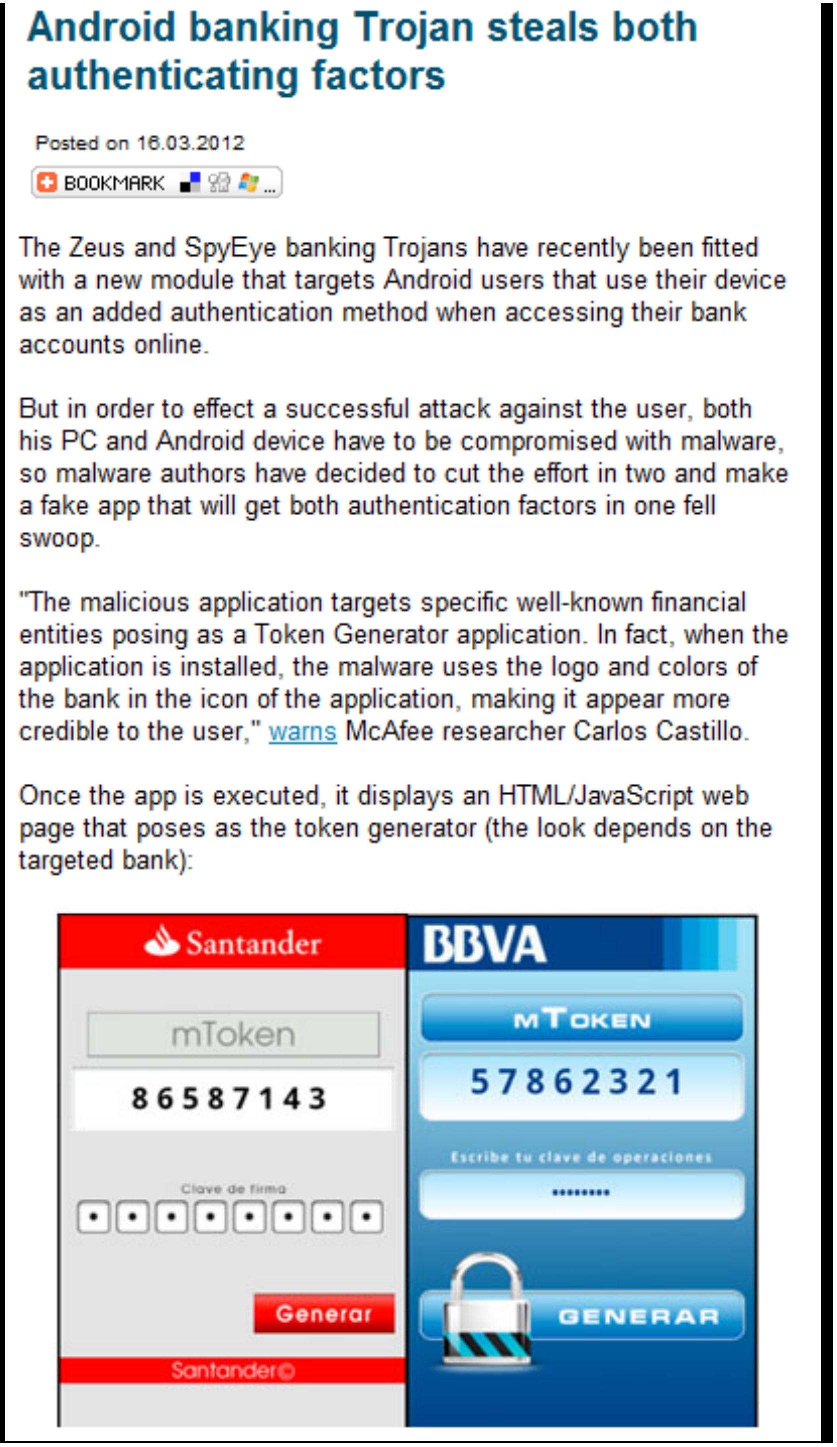
Please chose your phone's operating system:

○ iOS (iPhone)

ZitMo also targets Android users by means of a survey.

The ZeuS and SpyEye mobile bots have been updated!

http://www.net-security.org/malware_news.php?id=2037&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29



Android banking Trojan steals both authenticating factors

Posted on 16.03.2012

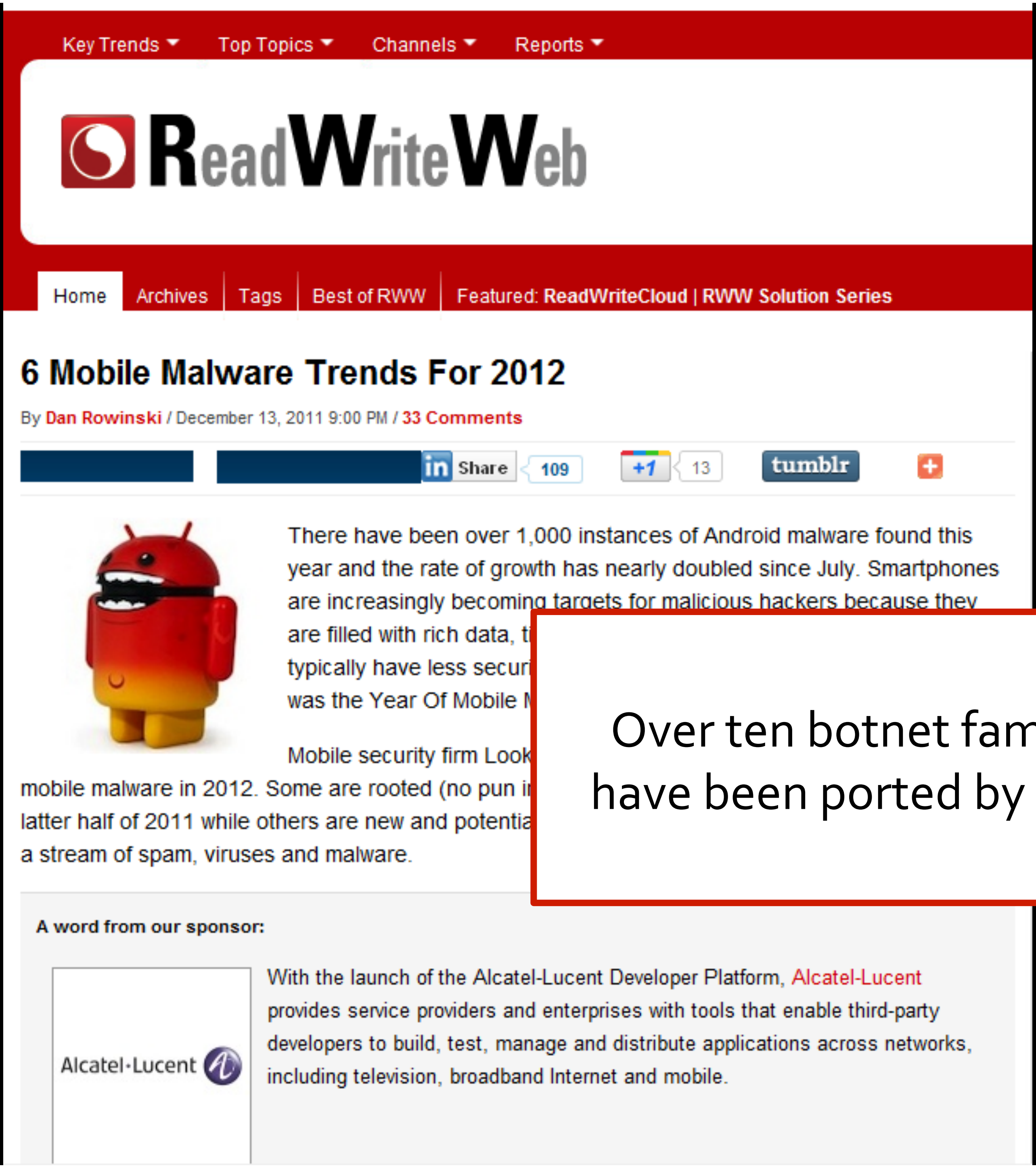
The Zeus and SpyEye banking Trojans have recently been fitted with a new module that targets Android users that use their device as an added authentication method when accessing their bank accounts online.

But in order to effect a successful attack against the user, both his PC and Android device have to be compromised with malware, so malware authors have decided to cut the effort in two and make a fake app that will get both authentication factors in one fell swoop.

"The malicious application targets specific well-known financial entities posing as a Token Generator application. In fact, when the application is installed, the malware uses the logo and colors of the bank in the icon of the application, making it appear more credible to the user," warns McAfee researcher Carlos Castillo.

Once the app is executed, it displays an HTML/JavaScript web page that poses as the token generator (the look depends on the targeted bank):

http://www.readwriteweb.com/archives/6_mobile_malware_predictions_for_2012.php



6 Mobile Malware Trends For 2012

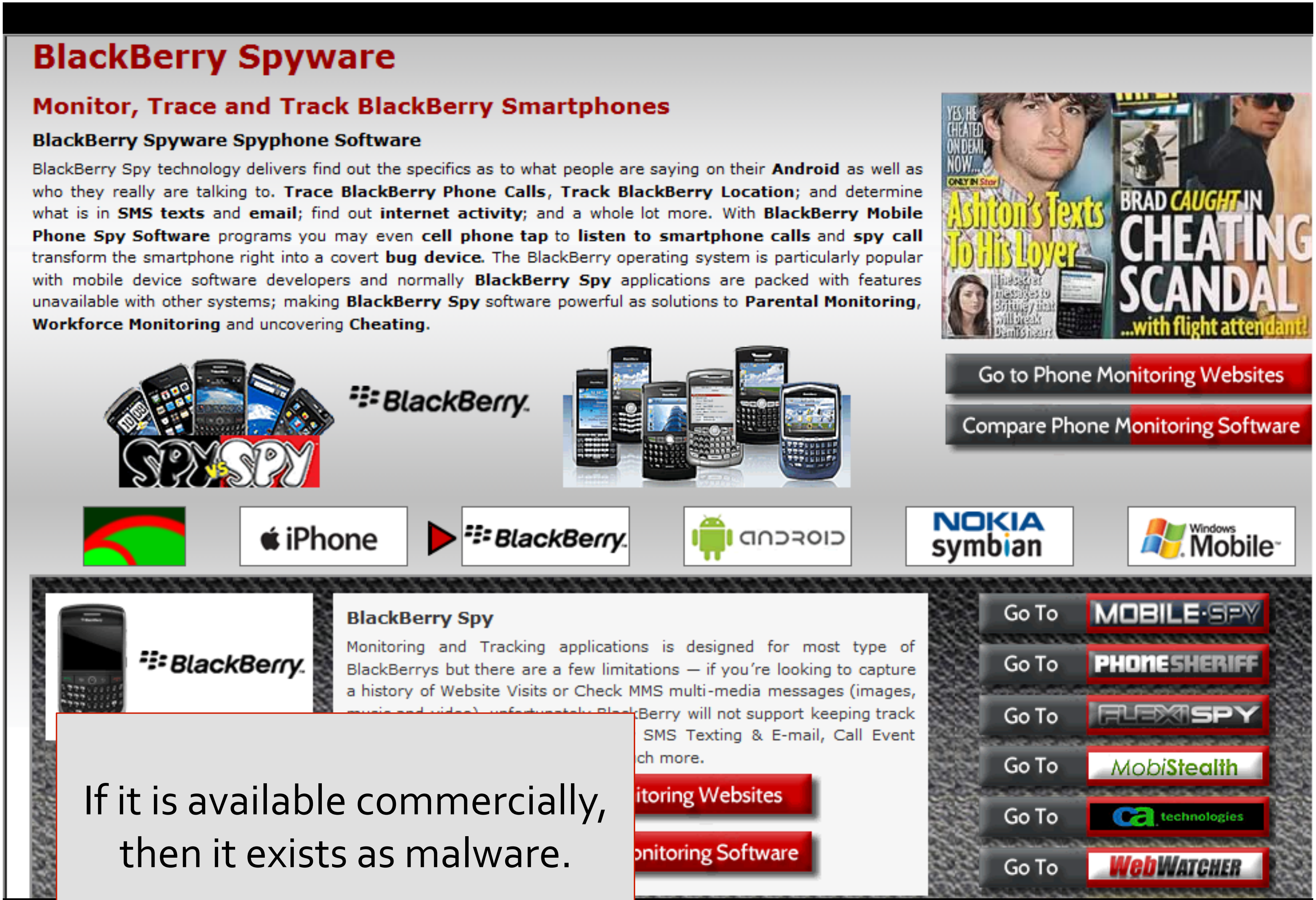
By Dan Rowinski / December 13, 2011 9:00 PM / 33 Comments

There have been over 1,000 instances of Android malware found this year and the rate of growth has nearly doubled since July. Smartphones are increasingly becoming targets for malicious hackers because they are filled with rich data, t
typically have less securi
was the Year Of Mobile M

Mobile security firm Look
mobile malware in 2012. Some are rooted (no pun i
latter half of 2011 while others are new and potentia
a stream of spam, viruses and malware.

Over ten botnet families have been ported by 2011.

Spyware – Malware and Commercial



BlackBerry Spyware

Monitor, Trace and Track BlackBerry Smartphones

BlackBerry Spyware Spyphone Software

BlackBerry Spy technology delivers find out the specifics as to what people are saying on their **Android** as well as who they really are talking to. **Trace BlackBerry Phone Calls**, **Track BlackBerry Location**; and determine what is in **SMS texts** and **email**; find out **internet activity**; and a whole lot more. With **BlackBerry Mobile Phone Spy Software** programs you may even **cell phone tap** to **listen to smartphone calls** and **spy call** transform the smartphone right into a covert **bug device**. The BlackBerry operating system is particularly popular with mobile device software developers and normally **BlackBerry Spy** applications are packed with features unavailable with other systems; making **BlackBerry Spy** software powerful as solutions to **Parental Monitoring**, **Workforce Monitoring** and uncovering **Cheating**.

YES, HE CHEATED ON DEMI NOW...
ONLY IN Star
Ashton's Texts To His Lover
The secret messages to Brittney that will break Demi's heart
BRAD CAUGHT IN CHEATING SCANDAL
...with flight attendant!
SPY vs SPY
BlackBerry
iPhone
BlackBerry
android
NOKIA symbian
Windows Mobile
BlackBerry

Go to Phone Monitoring Websites

Compare Phone Monitoring Software

BlackBerry Spy

Monitoring and Tracking applications is designed for most type of BlackBerrys but there are a few limitations — if you're looking to capture a history of Website Visits or Check MMS multi-media messages (images, music and video), unfortunately BlackBerry will not support keeping track … SMS Texting & E-mail, Call Event …ch more.

…itoring Websites

…onitoring Software

Go To MOBILE-SPY

Go To PHONESHERIFF

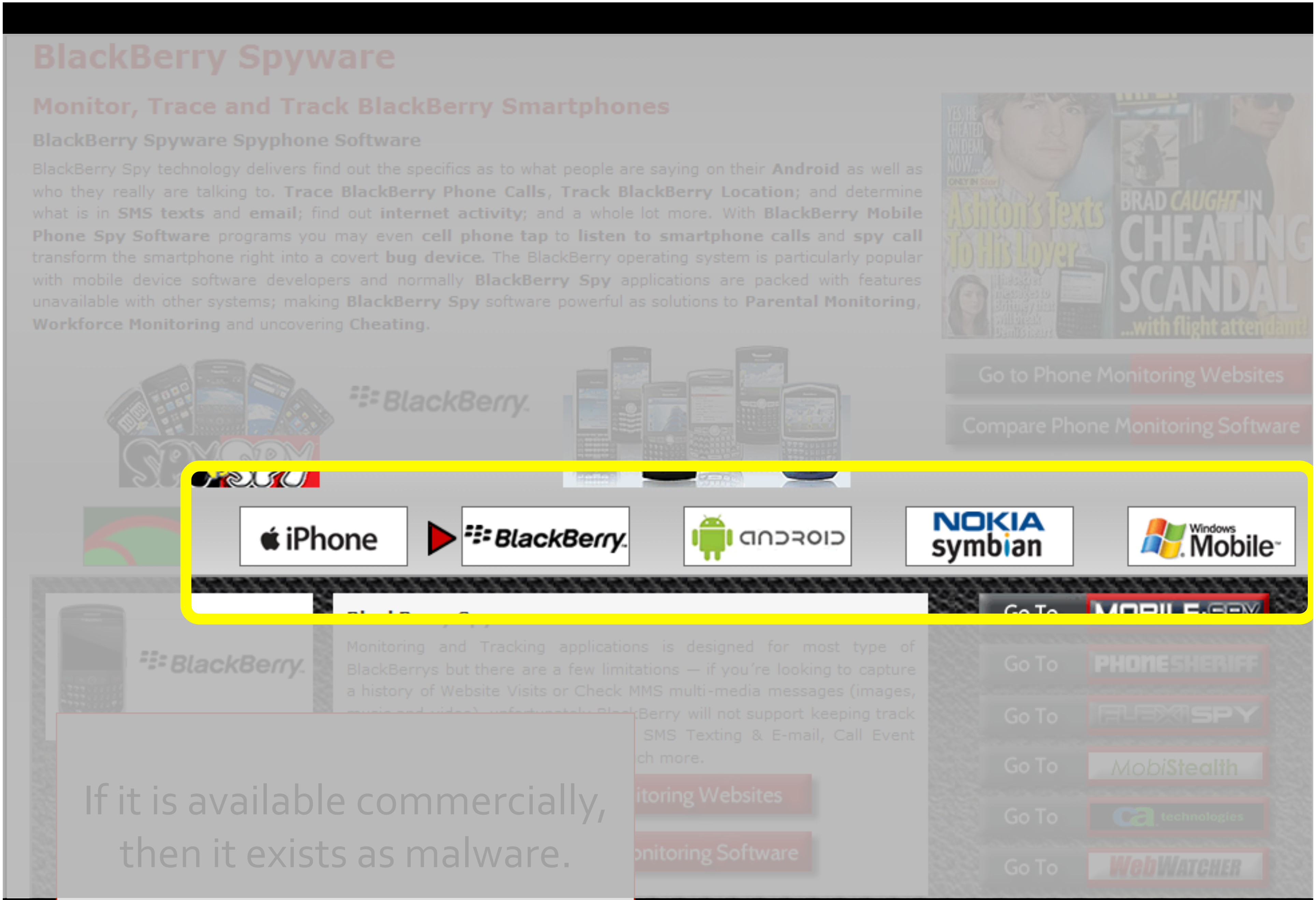
Go To FLEXISPY

Go To MobiStealth

Go To ca technologies

Go To WebWatcher

If it is available commercially, then it exists as malware.



BlackBerry Spyware

Monitor, Trace and Track BlackBerry Smartphones

BlackBerry Spyware Spyphone Software

BlackBerry Spy technology delivers find out the specifics as to what people are saying on their **Android** as well as who they really are talking to. **Trace BlackBerry Phone Calls**, **Track BlackBerry Location**; and determine what is in **SMS texts** and **email**; find out **internet activity**; and a whole lot more. With **BlackBerry Mobile Phone Spy Software** programs you may even **cell phone tap** to **listen to smartphone calls** and **spy call** transform the smartphone right into a covert **bug device**. The BlackBerry operating system is particularly popular with mobile device software developers and normally **BlackBerry Spy** applications are packed with features unavailable with other systems; making **BlackBerry Spy** software powerful as solutions to **Parental Monitoring**, **Workforce Monitoring** and uncovering **Cheating**.

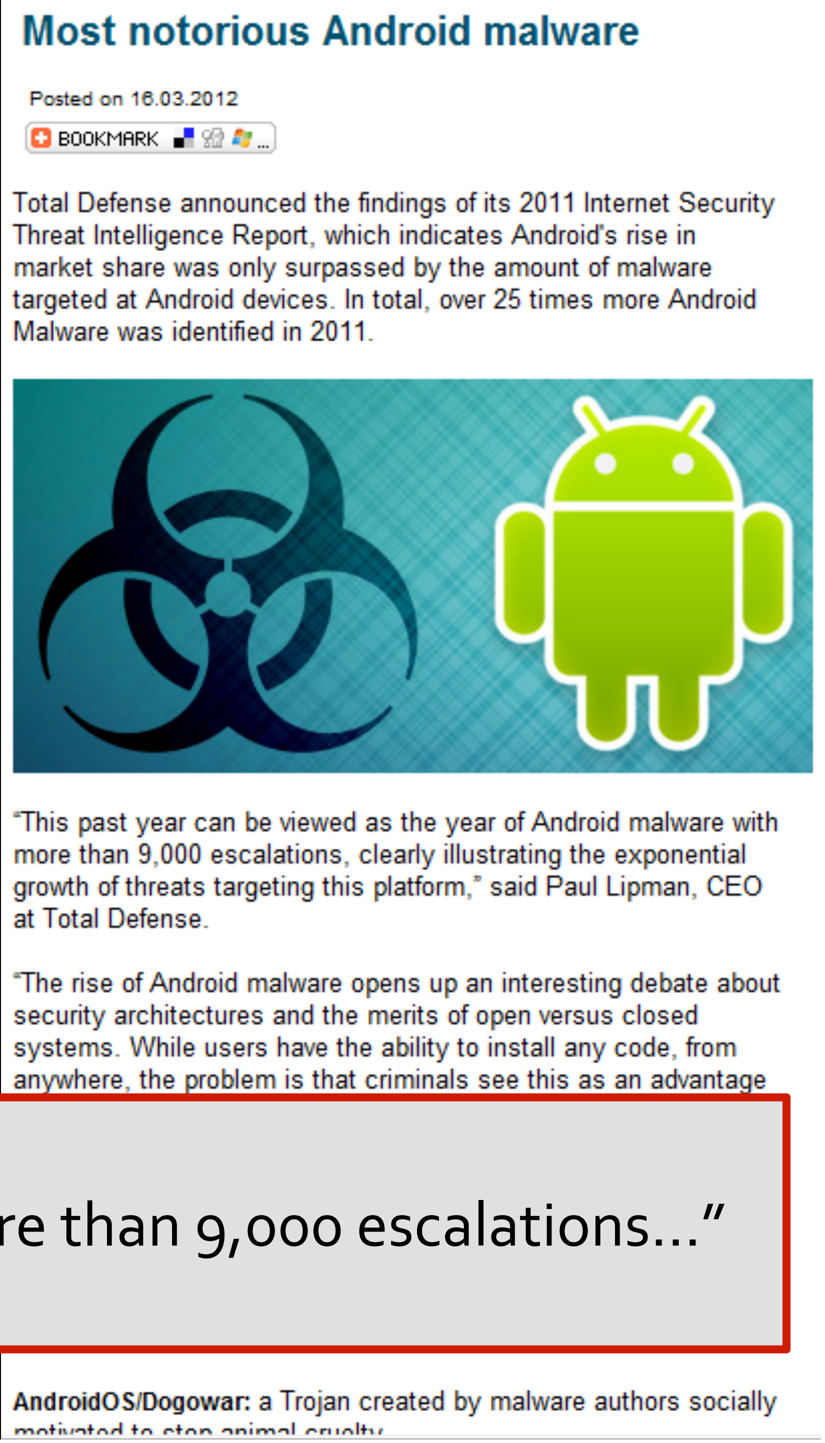
Monitoring and Tracking applications is designed for most type of BlackBerrys but there are a few limitations — if you're looking to capture a history of Website Visits or Check MMS multi-media messages (images, music and video), unfortunately BlackBerry will not support keeping track SMS Texting & E-mail, Call Event ch more.

If it is available commercially, then it exists as malware.

Total Defense's Report
(Released in March 2012)

Most notorious malware

- AndroidOS/Foncy SMS Trojan
- AndroidOS/Dogowar SMS Trojan
- AndroidOS/Fakeneflic.A Trojan-InfoStealer
- AndroidOS/WalkSteal.A SMS-Trojan
- AndroidOS/FakePlayer.A SMS-Trojan
- AndroidOS/Golddream.A Trojan-Monitor/Stealer



Most notorious Android malware

Posted on 16.03.2012

Total Defense announced the findings of its 2011 Internet Security Threat Intelligence Report, which indicates Android's rise in market share was only surpassed by the amount of malware targeted at Android devices. In total, over 25 times more Android Malware was identified in 2011.

"This past year can be viewed as the year of Android malware with more than 9,000 escalations, clearly illustrating the exponential growth of threats targeting this platform," said Paul Lipman, CEO at Total Defense.

"The rise of Android malware opens up an interesting debate about security architectures and the merits of open versus closed systems. While users have the ability to install any code, from anywhere, the problem is that criminals see this as an advantage

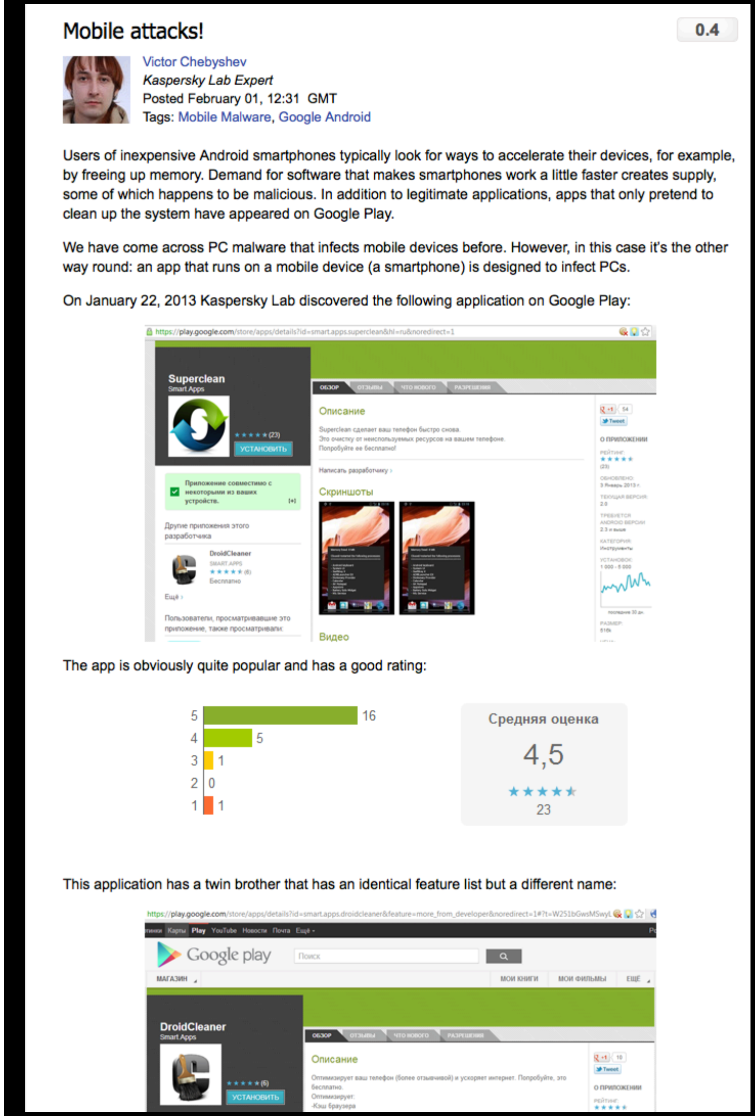
AndroidOS/Dogowar: a Trojan created by malware authors socially motivated to stop animal cruelty.

"…more than 9,000 escalations…"

http://www.net-security.org/malware_news.php?id=2035&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

Android is not alone.

A malicious app on a phone infects a PC.



Mobile attacks!

0.4

Victor Chebyshev
Kaspersky Lab Expert
Posted February 01, 12:31 GMT
Tags: Mobile Malware, Google Android

Users of inexpensive Android smartphones typically look for ways to accelerate their devices, for example, by freeing up memory. Demand for software that makes smartphones work a little faster creates supply, some of which happens to be malicious. In addition to legitimate applications, apps that only pretend to clean up the system have appeared on Google Play.

We have come across PC malware that infects mobile devices before. However, in this case it's the other way round: an app that runs on a mobile device (a smartphone) is designed to infect PCs.

On January 22, 2013 Kaspersky Lab discovered the following application on Google Play:

https://play.google.com/store/apps/details?id=smart.apps.superclean&hl=ru&noredirect=1

Superclean
Smart Apps
★★★★★ (23)
УСТАНОВИТЬ

ОБЗОР | ОТЗЫВЫ | ЧТО НОВОГО | РАЗРЕШЕНИЯ

Описание

Superclean сделает ваш телефон быстро снова.
Это очистку от неиспользуемых ресурсов на вашем телефоне.
Попробуйте ее бесплатно!

Написать разработчику ›

Скриншоты

Видео

Приложение совместимо с некоторыми из ваших устройств.

Другие приложения этого разработчика

DroidCleaner
SMART APPS
★★★★★ (6)
Бесплатно

Ещё ›

Пользователи, просматривавшие это приложение, также просматривали:

О ПРИЛОЖЕНИИ
РЕЙТИНГ: ★★★★★ (23)
ОБНОВЛЕНО: 3 Января 2013 г.
ТЕКУЩАЯ ВЕРСИЯ: 2.0
ТРЕБУЕТСЯ ANDROID ВЕРСИИ: 2.3 и выше
КАТЕГОРИЯ: Инструменты
УСТАНОВОК: 1 000 - 5 000
последние 30 дн.
РАЗМЕР: 516k

The app is obviously quite popular and has a good rating:

5	16
4	5
3	1
2	0
1	1

Средняя оценка
4,5
★★★★★
23

This application has a twin brother that has an identical feature list but a different name:

https://play.google.com/store/apps/details?id=smart.apps.droidcleaner&feature=more_from_developer&noredirect=1#?t=W251bGwsMSwyL

Карты | Play | YouTube | Новости | Почта | Ещё

Google play
Поиск

МАГАЗИН | МОИ КНИГИ | МОИ ФИЛЬМЫ | ЕЩЁ

DroidCleaner
Smart Apps
★★★★★ (6)
УСТАНОВИТЬ

ОБЗОР | ОТЗЫВЫ | ЧТО НОВОГО | РАЗРЕШЕНИЯ

Описание

Оптимизирует ваш телефон (более отзывчивой) и ускоряет интернет. Попробуйте, это бесплатно.
Оптимизирует:
-Кэш браузера

О ПРИЛОЖЕНИИ
РЕЙТИНГ: ★★★★★

DroidClean infects a PC.

http://www.securelist.com/en/blog/805/Mobile_attacks

Are you hands free?

Hands free?

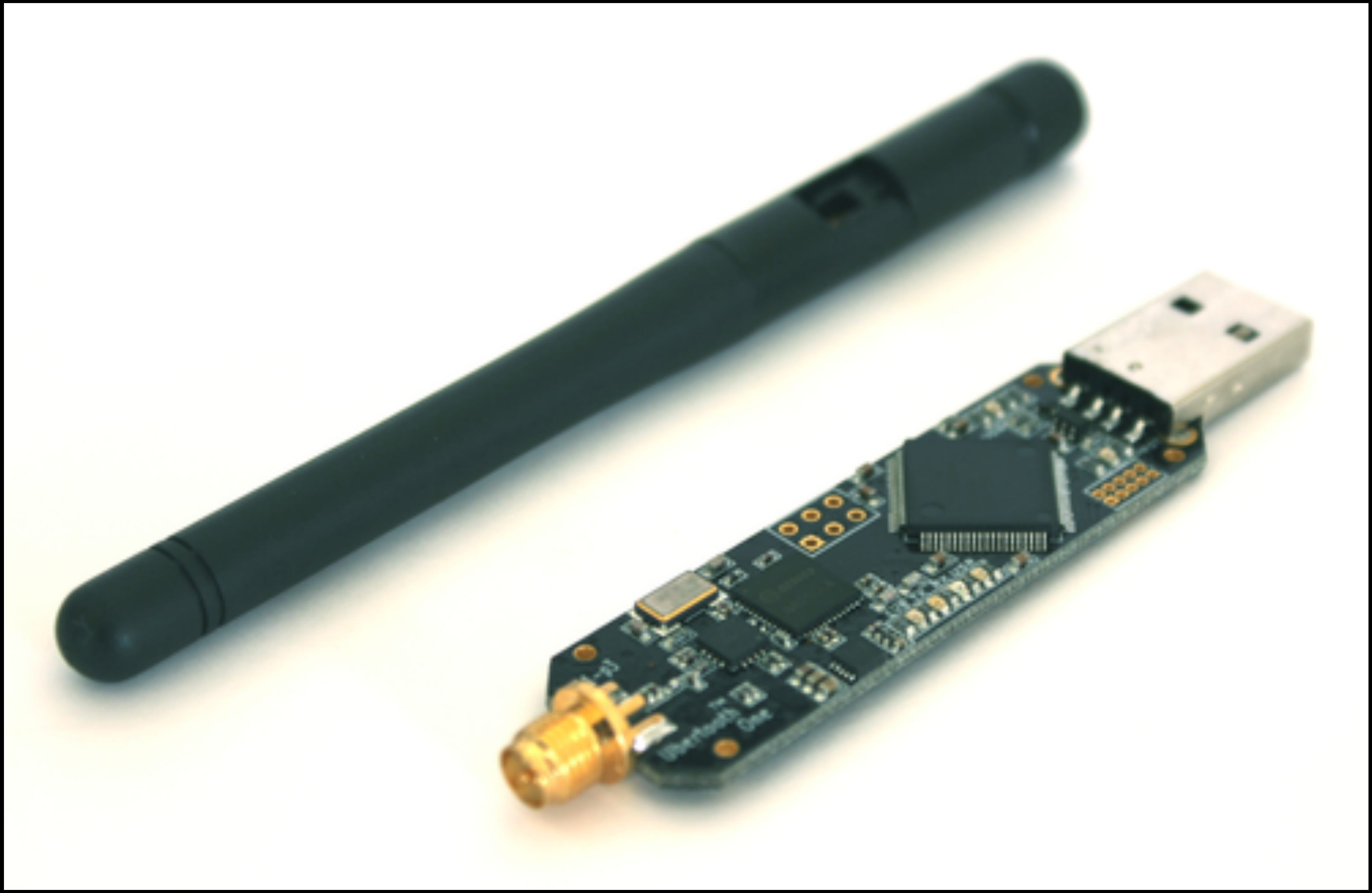
http://archshrk.com/cell-phones-new-law-2008

Not that “hands free.”

http://www.wellpromo.com/upload/upimg12/Bluetooth-Hands-Free-Headset-125812.jpg

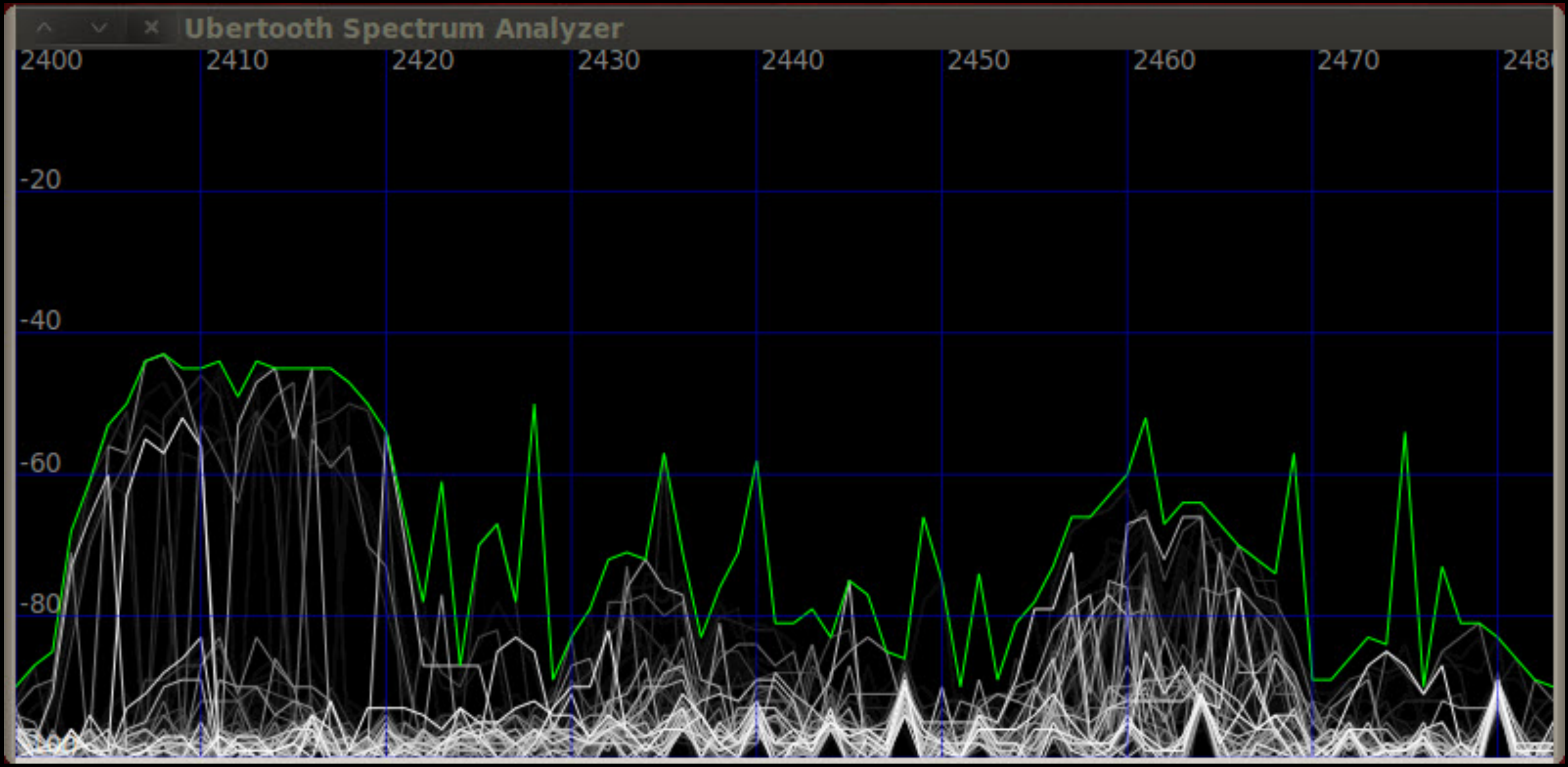
Let me introduce someone to you.

Meet the Ubertooth.



http://hackable-devices.org/shop/product/ubertooth-one

Scanning Bluetooth Traffic

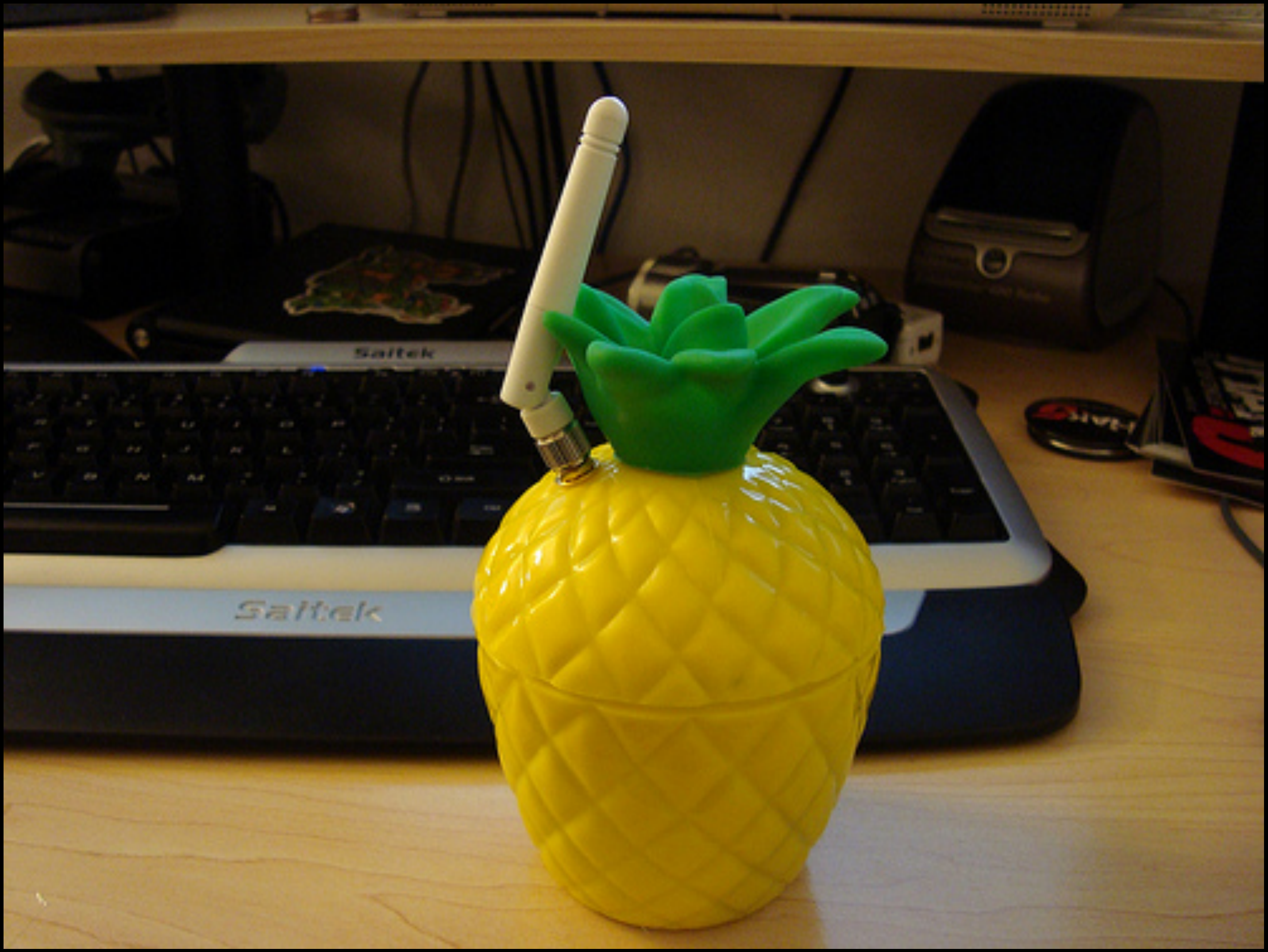


And then there is “free” wi-fi.

STARBUCKS
COFFEE
®

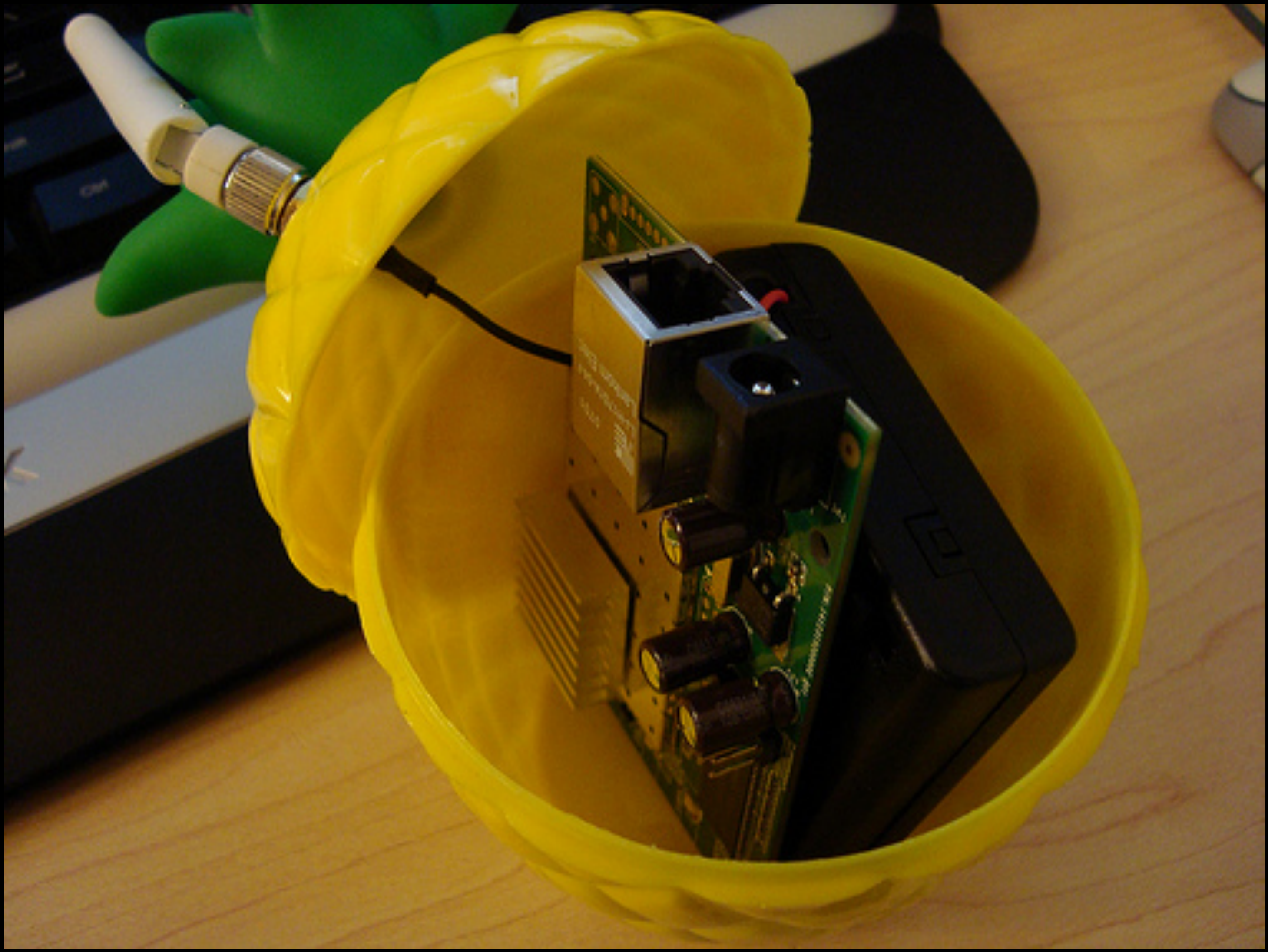
+

The Pineapple Router

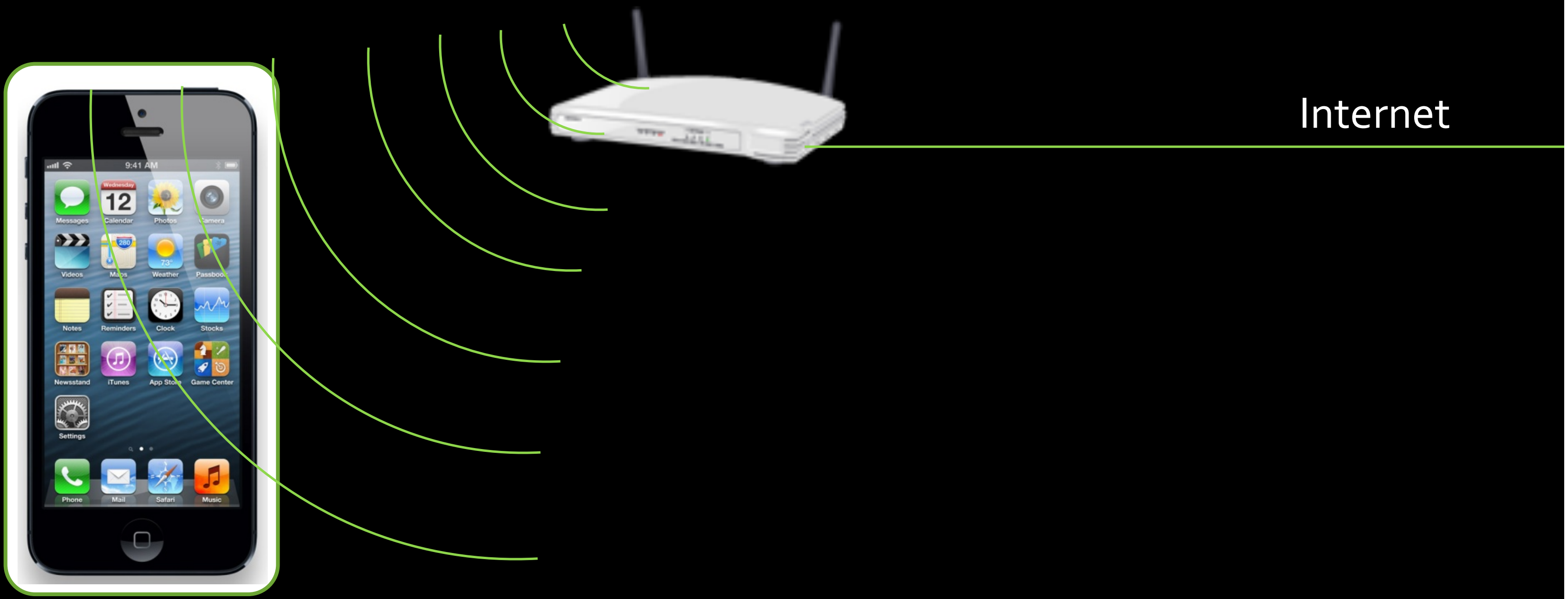


http://forums.hak5.org/index.php?showtopic=9903&st=20

The Pineapple Router

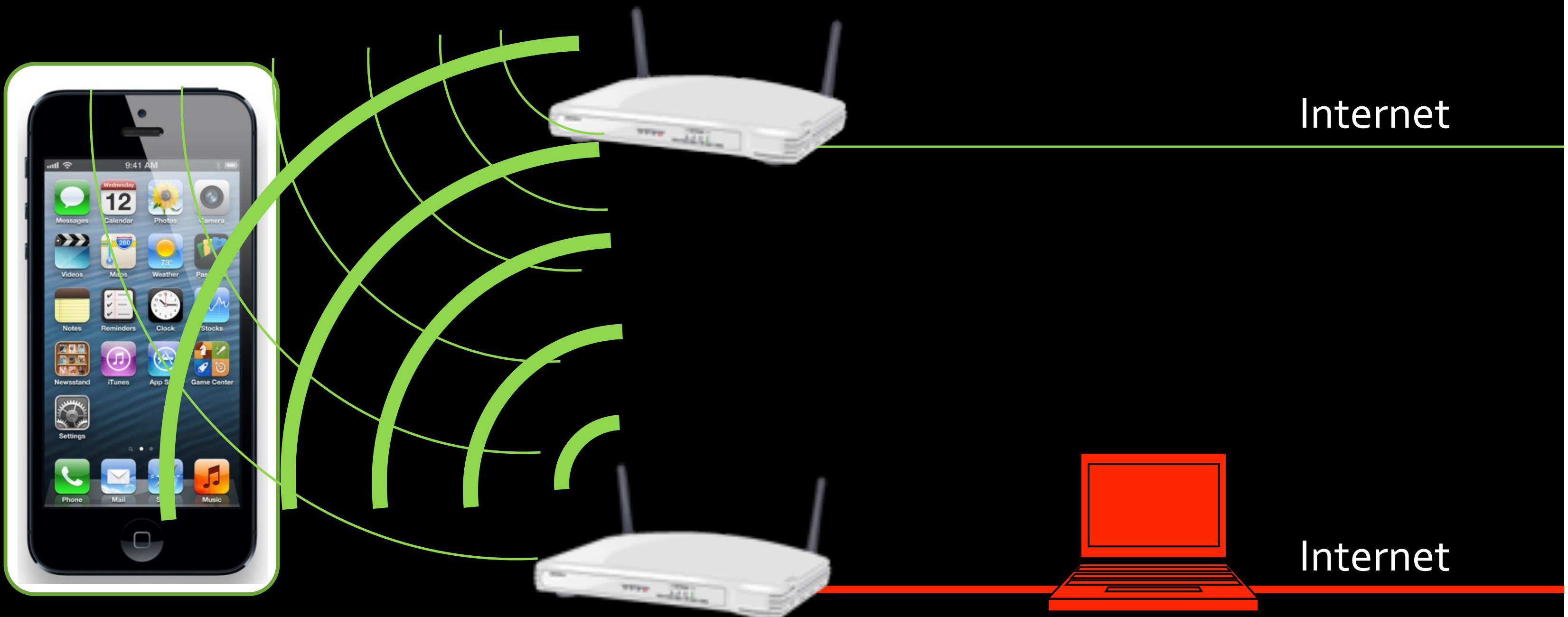


http://forums.hak5.org/index.php?showtopic=9903&st=20



Internet

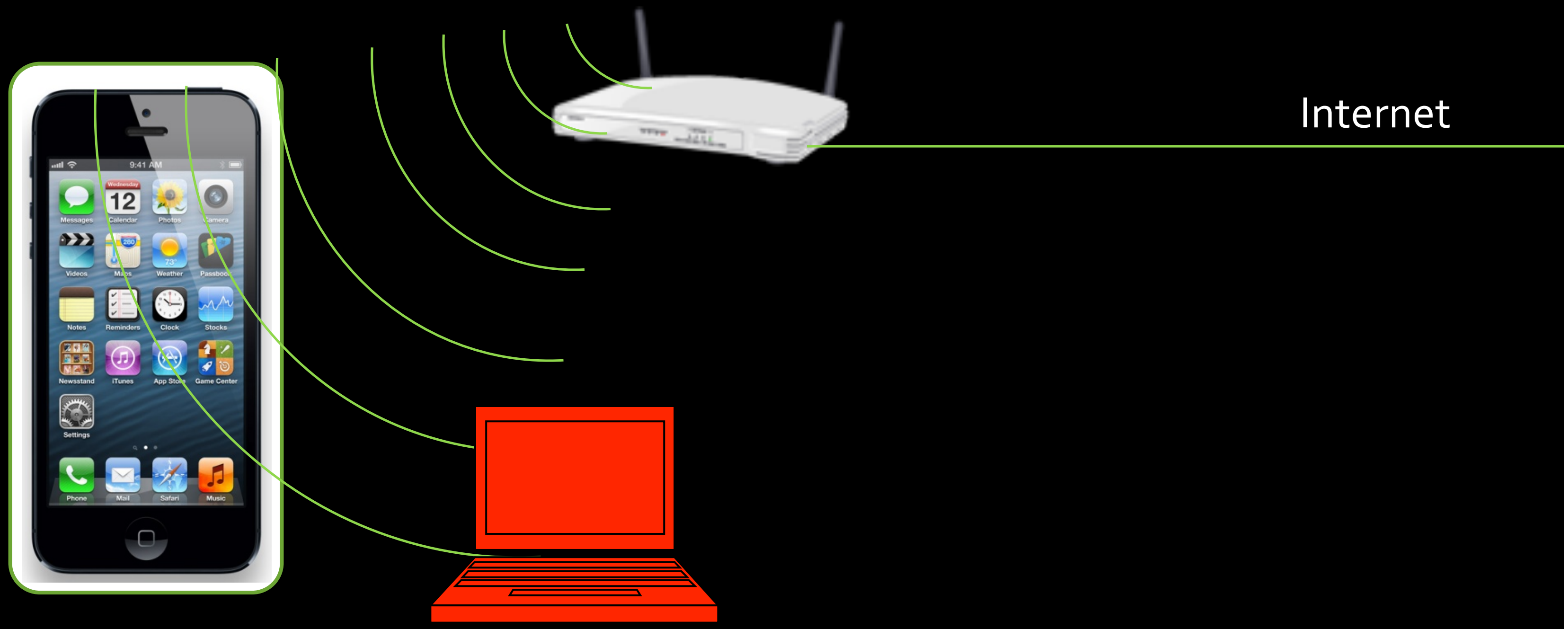
To whom would you listen?

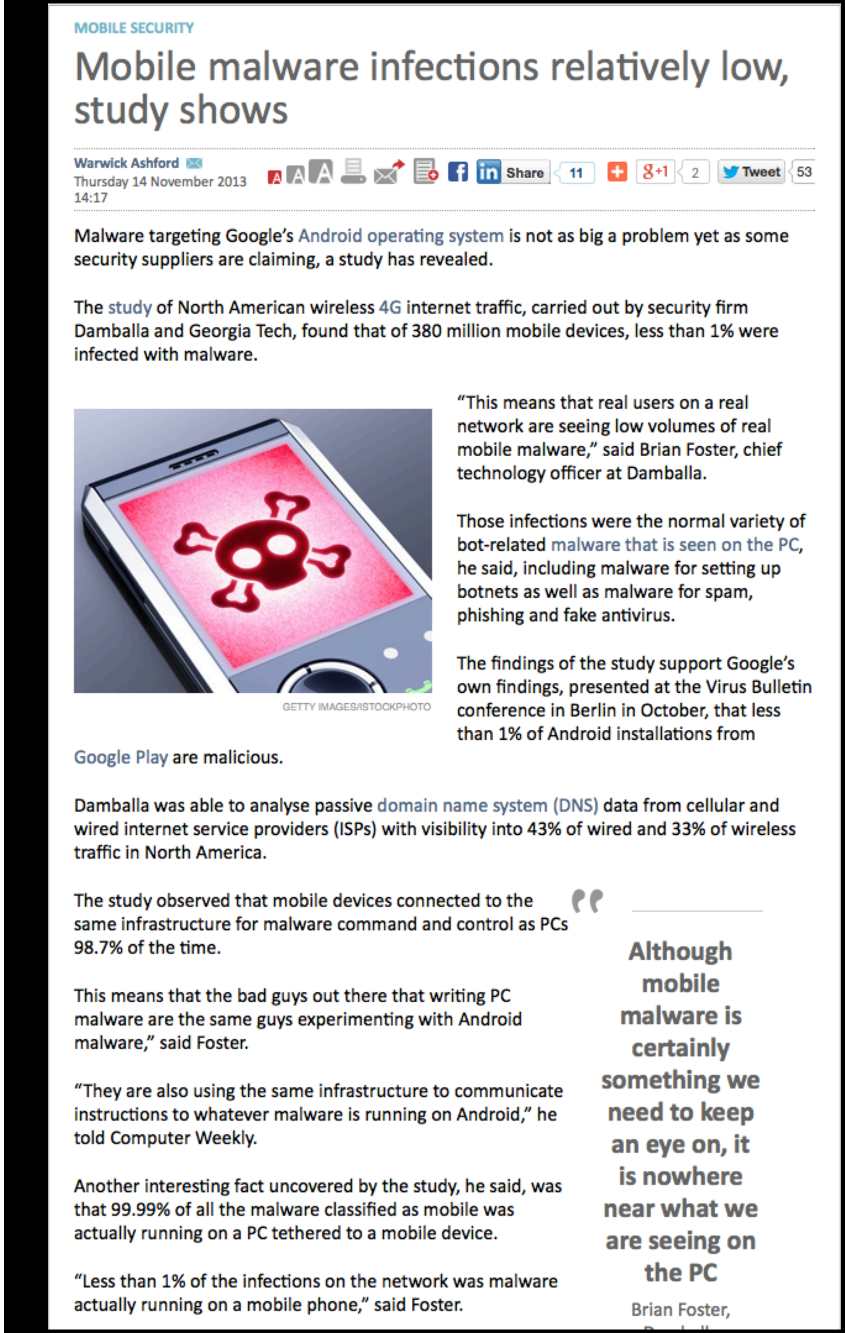


Internet

Internet

Sidejacking





MOBILE SECURITY

Mobile malware infections relatively low, study shows

Warwick Ashford
Thursday 14 November 2013
14:17

Malware targeting Google's Android operating system is not as big a problem yet as some security suppliers are claiming, a study has revealed.

The study of North American wireless 4G internet traffic, carried out by security firm Damballa and Georgia Tech, found that of 380 million mobile devices, less than 1% were infected with malware.

"This means that real users on a real network are seeing low volumes of real mobile malware," said Brian Foster, chief technology officer at Damballa.

Those infections were the normal variety of bot-related malware that is seen on the PC, he said, including malware for setting up botnets as well as malware for spam, phishing and fake antivirus.

The findings of the study support Google's own findings, presented at the Virus Bulletin conference in Berlin in October, that less than 1% of Android installations from Google Play are malicious.

GETTY IMAGES/ISTOCKPHOTO

Damballa was able to analyse passive domain name system (DNS) data from cellular and wired internet service providers (ISPs) with visibility into 43% of wired and 33% of wireless traffic in North America.

The study observed that mobile devices connected to the same infrastructure for malware command and control as PCs 98.7% of the time.

This means that the bad guys out there that writing PC malware are the same guys experimenting with Android malware," said Foster.

"They are also using the same infrastructure to communicate instructions to whatever malware is running on Android," he told Computer Weekly.

Another interesting fact uncovered by the study, he said, was that 99.99% of all the malware classified as mobile was actually running on a PC tethered to a mobile device.

"Less than 1% of the infections on the network was malware actually running on a mobile phone," said Foster.

> Although mobile malware is certainly something we need to keep an eye on, it is nowhere near what we are seeing on the PC
>
> Brian Foster,

Some say, "no."

Of North American 4G users, less than 1% of the 380,000,000 were infected.

That's about 3,800,000.

http://www.computerweekly.com/news/2240209033/Mobile-malware-infections-relatively-low-study-shows

How do we stop this?

MDMs are not enough.

Protect high profile users.

Consistent auditing (forensic analysis).

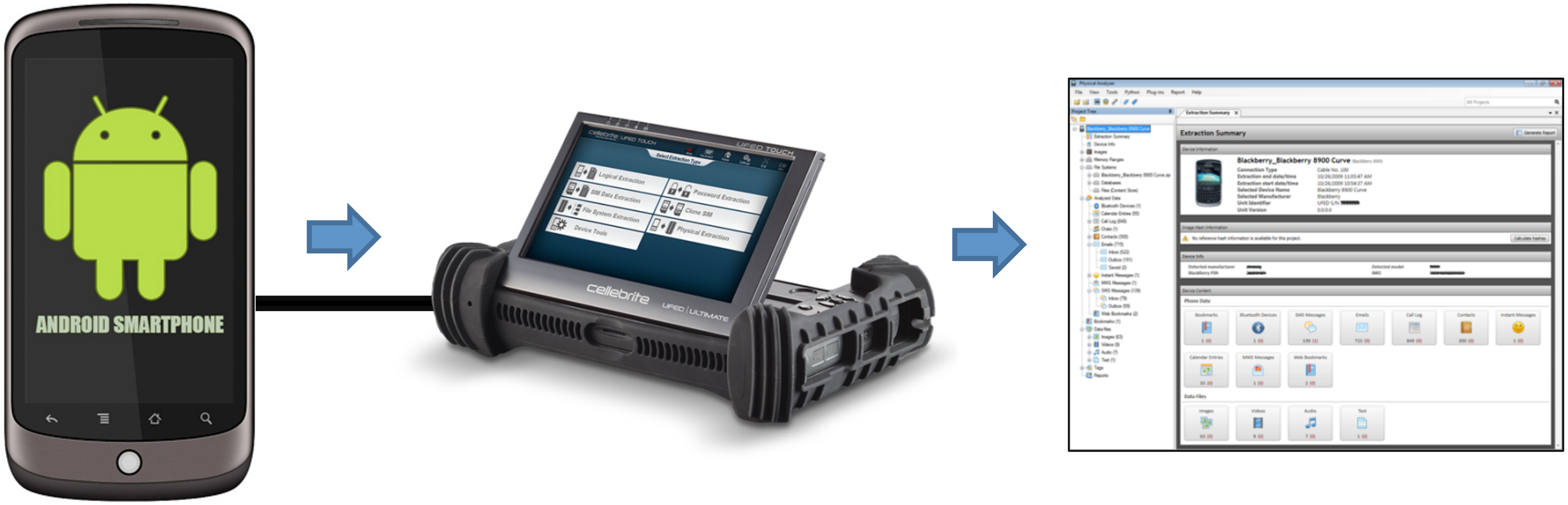
Analyze our apps the same way bad guys do.

Change user behavior.

How can we analyze this?

Conduct a physical acquisition and retrieve:

1. /Root/system/packages.xml
2. AndroidManifest.xml for the application
3. The application itself (.apk)

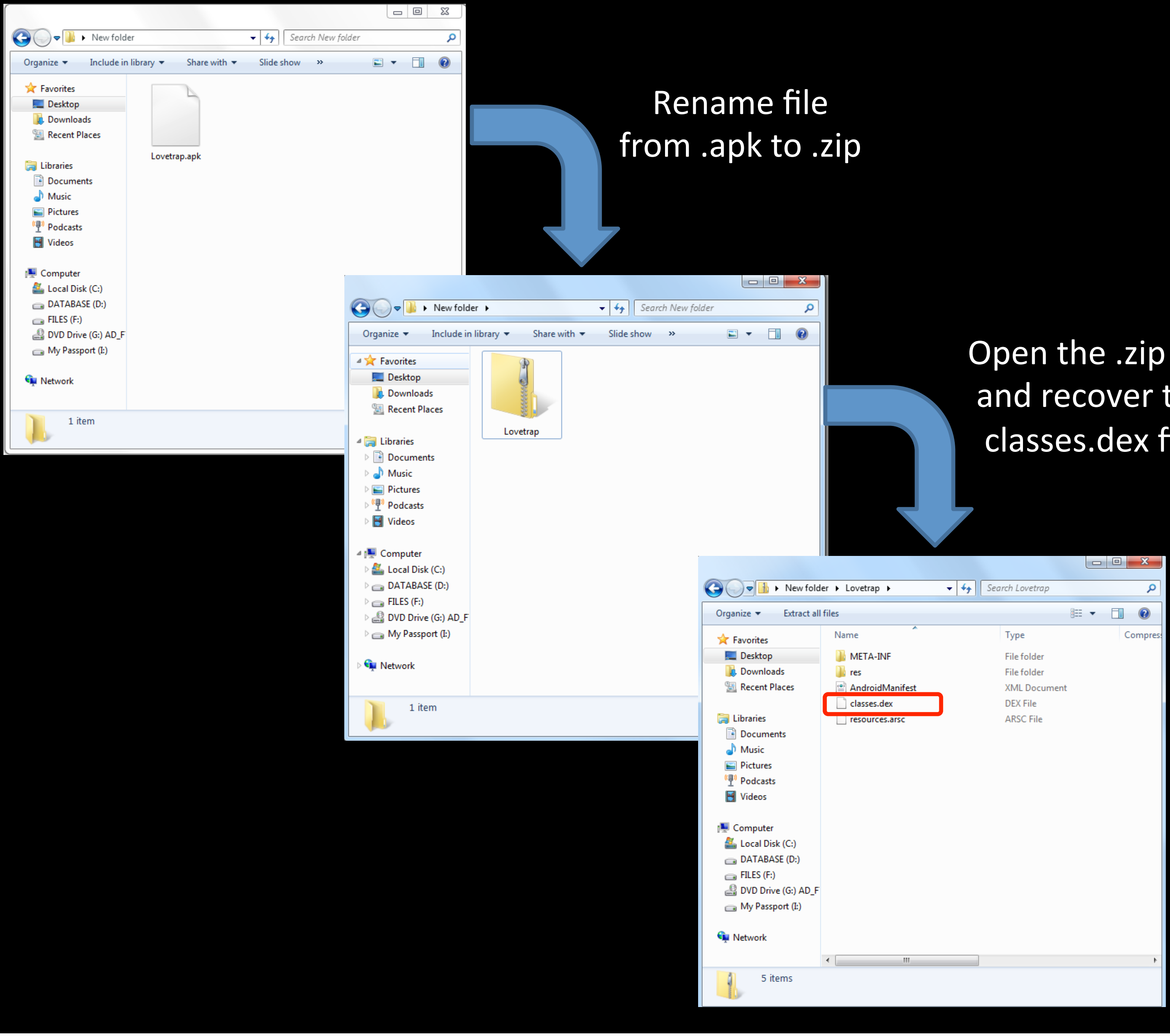


Packages.xml

- A list of applications and associated permissions

AndroidManifest.xml

- Names the Java package for the application. The package name serves as a unique identifier for the application.
- Describes the components of the application — the activities, services, broadcast receivers, and content providers that the application is composed of. It names the classes that implement each of the components and publishes their capabilities (for example, which Intent messages they can handle). These declarations let the Android system know what the components are and under what conditions they can be launched.
- Determines which processes will host application components.
- Declares which permissions the application must have in order to access protected parts of the API and interact with other applications.
- Declares the permissions that others are required to have in order to interact with the application's components.
- Lists the Instrumentation classes that provide profiling and other information as the application is running. These declarations are present in the manifest only while the application is being developed and tested; they're removed before the application is published.
- Declares the minimum level of the Android API that the application requires.
- Lists the libraries that the application must be linked against.



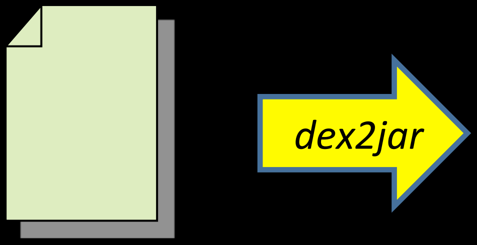
Rename file from .apk to .zip

Open the .zip file and recover the classes.dex file

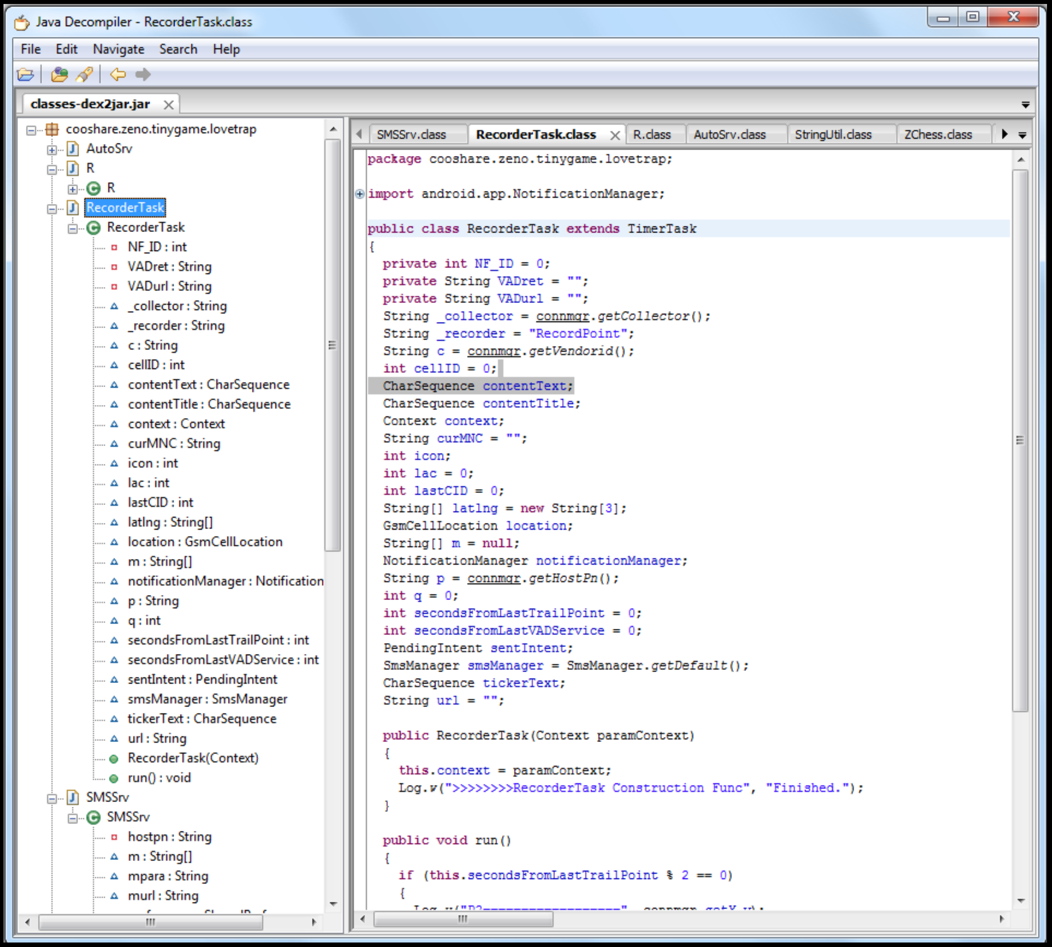
Name	Type	Compres
META-INF	File folder	
res	File folder	
AndroidManifest	XML Document	
classes.dex	DEX File	
resources.arsc	ARSC File	

Convert the classes.dex file to a .jar file and examine the contents.

Use a tool such as dex2jar. (http://code.google.com/p/dex2jar/)



classes.dex



```
cooshare.zeno.tinygame.lovetrap
  AutoSrv
  R
    R
  RecorderTask
    RecorderTask
      NF_ID : int
      VADret : String
      VADurl : String
      _collector : String
      _recorder : String
      c : String
      cellID : int
      contentText : CharSequence
      contentTitle : CharSequence
      context : Context
      curMNC : String
      icon : int
      lac : int
      lastCID : int
      latlng : String[]
      location : GsmCellLocation
      m : String[]
      notificationManager : Notification
      p : String
      q : int
      secondsFromLastTrailPoint : int
      secondsFromLastVADService : int
      sentIntent : PendingIntent
      smsManager : SmsManager
      tickerText : CharSequence
      url : String
      RecorderTask(Context)
      run() : void
  SMSSrv
    SMSSrv
      hostpn : String
      m : String[]
      mpara : String
      murl : String
```

```java
package cooshare.zeno.tinygame.lovetrap;

import android.app.NotificationManager;

public class RecorderTask extends TimerTask
{
  private int NF_ID = 0;
  private String VADret = "";
  private String VADurl = "";
  String _collector = connmgr.getCollector();
  String _recorder = "RecordPoint";
  String c = connmgr.getVendorid();
  int cellID = 0;
  CharSequence contentText;
  CharSequence contentTitle;
  Context context;
  String curMNC = "";
  int icon;
  int lac = 0;
  int lastCID = 0;
  String[] latlng = new String[3];
  GsmCellLocation location;
  String[] m = null;
  NotificationManager notificationManager;
  String p = connmgr.getHostPn();
  int q = 0;
  int secondsFromLastTrailPoint = 0;
  int secondsFromLastVADService = 0;
  PendingIntent sentIntent;
  SmsManager smsManager = SmsManager.getDefault();
  CharSequence tickerText;
  String url = "";

  public RecorderTask(Context paramContext)
  {
    this.context = paramContext;
    Log.v(">>>>>>>>RecorderTask Construction Func", "Finished.");
  }

  public void run()
  {
    if (this.secondsFromLastTrailPoint % 2 == 0)
    {
```

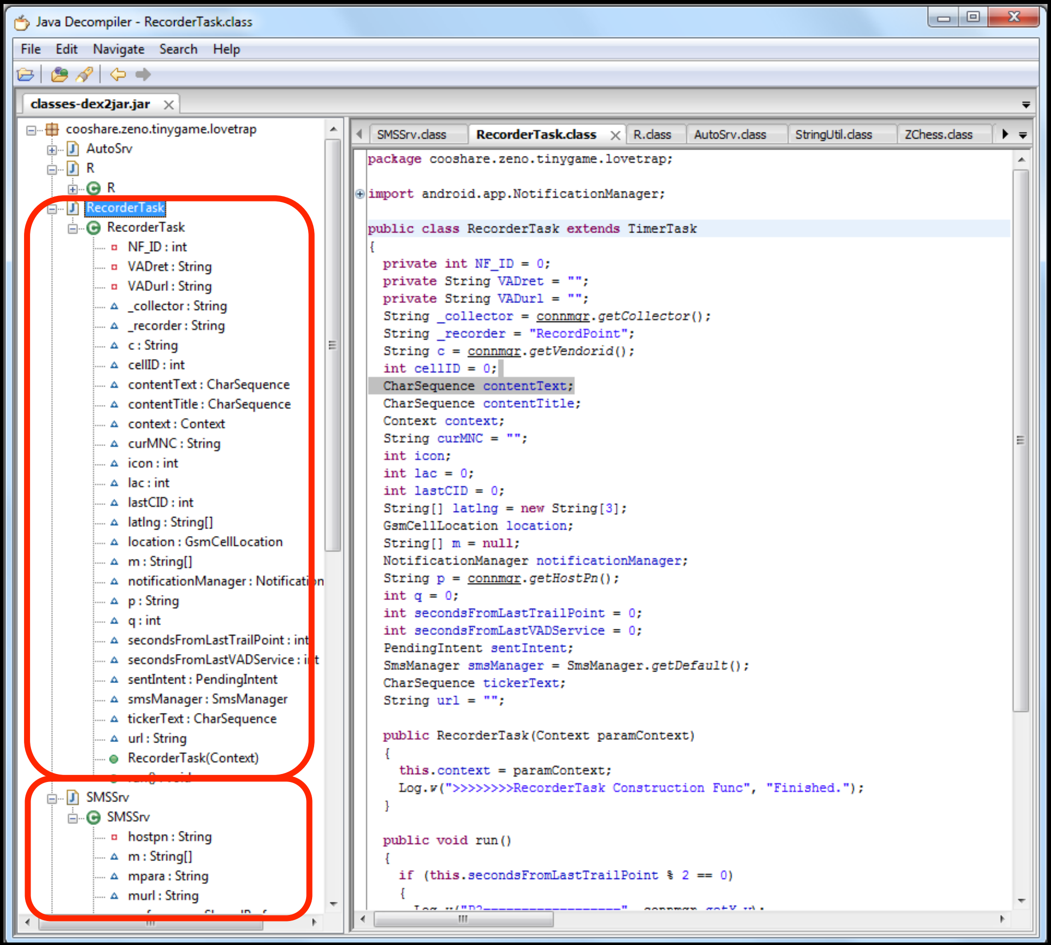
classes.jar

Lovetrap.apk

LoveTrap is an Android trojan that sends SMS messages to premium rate numbers.

The app retrieves premium rate numbers from a remote server in order to send the SMS messages that will be charged to the mobile user's account.

The trojan will attempt to go further and block any incoming confirmation SMS messages from any of the premium rate numbers in order to mask its activities.



```
cooshare.zeno.tinygame.lovetrap
  AutoSrv
  R
    R
  RecorderTask
    RecorderTask
      NF_ID : int
      VADret : String
      VADurl : String
      _collector : String
      _recorder : String
      c : String
      cellID : int
      contentText : CharSequence
      contentTitle : CharSequence
      context : Context
      curMNC : String
      icon : int
      lac : int
      lastCID : int
      latlng : String[]
      location : GsmCellLocation
      m : String[]
      notificationManager : Notificati n
      p : String
      q : int
      secondsFromLastTrailPoint : int
      secondsFromLastVADService : i t
      sentIntent : PendingIntent
      smsManager : SmsManager
      tickerText : CharSequence
      url : String
      RecorderTask(Context)
  SMSSrv
    SMSSrv
      hostpn : String
      m : String[]
      mpara : String
      murl : String
```

```
package cooshare.zeno.tinygame.lovetrap;

import android.app.NotificationManager;

public class RecorderTask extends TimerTask
{
  private int NF_ID = 0;
  private String VADret = "";
  private String VADurl = "";
  String _collector = connmgr.getCollector();
  String _recorder = "RecordPoint";
  String c = connmgr.getVendorid();
  int cellID = 0;
  CharSequence contentText;
  CharSequence contentTitle;
  Context context;
  String curMNC = "";
  int icon;
  int lac = 0;
  int lastCID = 0;
  String[] latlng = new String[3];
  GsmCellLocation location;
  String[] m = null;
  NotificationManager notificationManager;
  String p = connmgr.getHostPn();
  int q = 0;
  int secondsFromLastTrailPoint = 0;
  int secondsFromLastVADService = 0;
  PendingIntent sentIntent;
  SmsManager smsManager = SmsManager.getDefault();
  CharSequence tickerText;
  String url = "";

  public RecorderTask(Context paramContext)
  {
    this.context = paramContext;
    Log.v(">>>>>>>>RecorderTask Construction Func", "Finished.");
  }

  public void run()
  {
    if (this.secondsFromLastTrailPoint % 2 == 0)
    {
```

classes.jar

michael.robinson@disruptive-sol.com

Why we are failing and how we can fix this

MOBILE DEVICES